

User Guide

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Contents

Product Overview

LED panel 2
Ports panel 3

Wireless Security Checklist

Change the default wireless network name or SSID 4
Change the default password 4
Enable MAC address filtering 4
Enable encryption 4

General Network Security Guidelines 4
Additional Security Tips 5

Advanced Configuration

How to access the browser-based utility 6
Setup > Basic Setup 7
Language 7
Network Setup 7
Wireless > Basic Wireless Settings 7
Basic Wireless Settings 8
Wireless Security 8
Wi-Fi Protected Setup 9
Wireless > Wireless Network Site Survey 10
Wireless Network Site Survey 10
Wireless > WMM® 11
WMM 12
Wireless > Advanced Wireless Settings 13
Advanced Wireless 13
Administration > Management 14
Management 14
Administration > Factory Defaults 15
Factory Defaults 15
Administration > Upgrade Firmware 15
Upgrade Firmware 15
Status > Bridge 15
Bridge Information 16
Local Network 16
Status > Wireless 16
Wireless 16

Troubleshooting

WES610N/WET610N 17

Specifications

WES610N 18
WET610N 19

Product Overview

Thank you for choosing the Linksys Dual-Band N Entertainment Bridge. The bridge can connect any wired, Ethernet device to your wireless network. The bridge is based on dual-band Wireless-N, so it is compatible with any Wireless-N, -G, -A, or -B router or access point. For first-time installation, follow the steps on the CD folder. To configure advanced settings, use the convenient, browser-based utility.

LED panel



WES610N WET610N

Wireless (Blue) The Wireless LED lights up when there is a wireless connection. The LED flashes when the bridge is actively sending or receiving data over the wireless network.

Wi-Fi Protected Setup Button If your router supports Wi-Fi Protected Setup and uses WPA or WPA2 security, then you can use Wi-Fi Protected Setup to automatically connect the bridge. To use Wi-Fi Protected Setup, refer to "Wireless > Basic Wireless Settings" on page 7.

Wi-Fi Protected Setup LED (Blue/Amber) The LED flashes blue for two minutes during Wi-Fi Protected Setup. It lights up blue when wireless security is enabled. If there is an error during the Wi-Fi Protected Setup process, then the LED lights up amber. Make sure the network router supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.

Ethernet (Blue) The Ethernet LED lights up when there is a wired connection. The LED flashes when the bridge is actively sending or receiving data over the Ethernet port(s).

Power (Blue) The Power LED lights up when the bridge is powered on.

Ports panel



WES610N WET610N

Ethernet The Ethernet port(s) connects the bridge to a computer or other Ethernet network device. The WES610N has four ports, and the WET610N has a single port.

Reset There are two ways to reset the bridge's factory defaults. Either press and hold the Reset button for approximately five seconds, or restore the defaults from Administration > Factory Defaults in the bridge's browser-based utility. The WES610N has a reset button on the bottom, and the WET610N has a reset button on the back port panel.

Power The Power port connects the bridge to the included power adapter.

Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use **linksys** as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

Change the default password

For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Linksys default password is **admin**. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.

Enable MAC address filtering

Linksys routers give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.

Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalent Privacy (WEP) offer different levels of security for wireless communication.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

Advanced Configuration

After setting up the bridge by following the steps on the CD folder, the bridge will be ready for use. However, if you want to change its advanced settings, use the bridge's browser-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer networked with the bridge.

The browser-based utility has these main tabs: Setup, Wireless, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

How to access the browser-based utility

Use a web browser to access the browser-based utility.

If the bridge is connected to a network with a DHCP server (usually the network router), then the bridge will obtain its IP address from the DHCP server. If there is no DHCP server, then the bridge will use its default static IP address, **169.254.1.250**. (If you set a permanent static IP address on the bridge through the browser-based utility, then enter the static IP address instead.)

NOTE
If you do not know the bridge's IP address, then find its IP address in the DHCP clients table of your router. (Refer to the documentation for your router.)

If you cannot locate the bridge's IP address, you can reset the bridge; press the **Reset** button on the bridge for approximately five seconds, using a straightened paper clip. This will reset the bridge back to the factory default settings. The bridge will request an IP address from the DHCP server (usually the network router). If no DHCP server is found, then the bridge will use its default static IP address, **169.254.1.250**, until it detects a DHCP server and is assigned a dynamic IP address.

If the bridge is not associated with a router and is using the factory default settings, connect a computer to the bridge using an Ethernet connection to access the web-based utility. You will need to configure the Ethernet connection on the computer with a static IP address and subnet mask.

The IP address of your Ethernet adapter should be set to a specific IP address.

1. In the *IP address* field, enter **169.254.x.y** (x should be replaced by a number between 1 and 254, and y should be replaced by a number between 0 and 255).
2. In the *Subnet mask* field, enter **255.255.0.0**.

NOTE
The steps to assign a static IP address to the Ethernet adapter on your computer vary by operating system. For instructions, please refer to the help documentation of your specific operating system.

After you have assigned your Ethernet adapter with a static IP address, launch your web browser, and enter the Adapter's IP address (the default setting is **169.254.1.250**)in the *Address* field. Press **Enter**.

A password request screen appears. (Non-Windows XP users will see a similar screen.) Leave the *User name* field blank. Enter the password you created during the Setup Wizard. If you did not create a new password, use the default password **admin**. (You can set a new password from the *Administration* > *Management* screen.) Click **OK** to continue.



NOTE
If the password request screen does not appear, wait two minutes and try again.

Setup > Basic Setup

The first screen that appears is the *Basic Setup* screen. Use this screen to change the browser-based utility's language, or to change the bridge's wired, Ethernet network settings.





Language

Language This is used to set the language displayed by the browser-based utility. Select the desired language from the drop-down menu.

Network Setup

This section determines if the bridge's IP address is obtained automatically from a DHCP server, such as your network router (Automatic Configuration - DHCP), or set manually (Static IP).

Bridge IP If your network has a DHCP server, such as your network router, assigning IP addresses to your network devices, then keep the default, **Automatic Configuration - DHCP**. The bridge will request an IP address from the DHCP server (usually the network router). If no DHCP server is found, then the bridge will use its default static IP address, **169.254.1.250**, until it detects a DHCP server and is assigned a dynamic IP address.

If you want to set a permanent static IP address for the bridge, then select **Static IP**.

If you select Static IP, then complete the following fields:

- **Static IP Address** Enter a unique IP address that will be used to access the browser-based utility.
- **Subnet Mask** Enter the subnet mask of your wired network.
- **Default Gateway** Enter the IP address of the default gateway for your network (in most cases, this is your router).

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Basic Wireless Settings

Use the *Basic Wireless Settings* screen to configure the bridge's basic wireless and security settings.

There are two ways to configure the bridge's settings, manual and Wi-Fi Protected Setup. Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If your network router supports Wi-Fi Protected Setup and uses WPA or WPA2 security, then you can use Wi-Fi Protected Setup to automatically connect the bridge.

Configuration View To manually configure your wireless network, select **Manual**. Refer to **Basic Wireless Settings**, **page 8**. To use Wi-Fi Protected Setup, select **Wi-Fi Protected Setup**. Refer to **Wi-Fi Protected Setup**, **page 9**.

Basic Wireless Settings



Network Name (SSID) The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any characters on the keyboard). Make sure this setting matches the setting on your wireless router or access point. For added security, you should change the default SSID (**linksys**) to a unique name.

Wireless Security

The bridge supports the following wireless security options: WPA Personal, WPA2 Personal, and WEP. WPA (Wi-Fi Protected Access) and WPA2 are stronger security methods than WEP (Wired Equivalent Privacy). For more information about wireless security, refer to "Wireless Security Checklist" on page 4.

Security Mode

Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

NOTE
Remember that each device in your wireless network MUST use the same security method and passphrase/key, or else the wireless devices will not be able to communicate with each other.

WPA Personal

WPA is a security standard stronger than WEP encryption.



Encryption WPA supports the TKIP encryption method, with dynamic encryption keys.

Passphrase Enter the key shared by the bridge and your wireless router or access point. It must have 8-63 characters.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

WPA2 Personal

WPA2 is a more advanced, more secure version of WPA.



Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the encryption method, **AES** or **TKIP or AES**. The default selection is **AES**.

Passphrase Enter the key shared by the bridge and wireless router or access point. It must have 8-63 characters.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

WEP

WEP is a basic encryption method, which is not as secure as WPA or WPA2.



Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**. The default is **40/64 bits (10 hex digits)**.

Key 1 Enter the WEP key of your network.

Tx Key **Key 1** is the transmit key used by the bridge.

Authentication The default is **Auto**, which allows either Open system or Shared key authentication to be used. Select **Open** to use open system authentication; the sender and recipient do not use a WEP key for authentication. Select **Shared** to use shared key authentication; the sender and recipient use a WEP key for authentication.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wi-Fi Protected Setup

There are two methods available. Use the method that applies to the router you are using.





Method #1

Use this method if your router has a Wi-Fi Protected Setup button.

1. Click or press the **Wi-Fi Protected Setup** button on the router.
2. Within two minutes, click the **Wi-Fi Protected Setup** button on the bridge's *Wi-Fi Protected Setup* screen.
3. After the bridge has been configured, click **Close**.

The *Wi-Fi Protected Setup* screen displays the Link Status, Network Name (SSID), and Security method.

Method #2

Use this method if your router requests the PIN number of the bridge.

1. On the **router's** *Wi-Fi Protected Setup* screen, enter the PIN number on the **bridge's** *Wi-Fi Protected Setup* screen. Then click **Register** or the appropriate button. (It is also listed on the label on the bottom of the bridge.)
2. On the **bridge's** *Wi-Fi Protected Setup* screen, click **OK**.
3. After the bridge has been configured, click **Close**.

The *Wi-Fi Protected Setup* screen displays the Link Status, Network Name (SSID), and Security method.

Wireless > Wireless Network Site Survey

Click the **Wireless Network Site Survey** tab to begin a site survey. The *Wireless Network Site Survey* screen lists the wireless networks detected by the bridge.



Wireless Network Site Survey

Number of Wireless Networks The number of wireless networks detected by the bridge is displayed.

Select To connect to a wireless network, click **Select**. Then click **Connect**.

Wireless Network Name The network name or SSID of the wireless network is displayed.

GHz The radio band of the wireless network is displayed.

Signal The percentage of signal strength is displayed. 100% is the strongest signal strength possible; 0% is the weakest possible.

Security If the network supports Wi-Fi Protected Setup, the Wi-Fi Protected Setup icon is displayed. The security method used by the wireless network is displayed.

Click **Refresh** to update the on-screen information.

After you have selected a network, click **Connect**. A new screen appears. Follow the instructions for the security method of your network.

WPA



Network Name (SSID) The name of the network you selected is automatically displayed.

Security Mode WPA Personal is automatically displayed.

Encryption WPA supports the TKIP encryption method, with dynamic encryption keys.

Passphrase Enter the key shared by the bridge and wireless router or access point. It must have 8-63 characters.

Click **Refresh** to update the on-screen information.

After you have entered the security settings, click **Connect**.

WPA2



Network Name (SSID) The name of the network you selected is automatically displayed.

Security Mode WPA2 Personal is automatically displayed.

Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the encryption method, **AES** or **TKIP or AES**.

Passphrase Enter the key shared by the bridge and wireless router or access point. It must have 8-63 characters.

Click **Refresh** to update the on-screen information.

After you have entered the security settings, click **Connect**.

WEP



Network Name (SSID) The name of the network you selected is automatically displayed.

Security Mode WEP is automatically displayed.

Encryption Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**.

Key 1 Enter the WEP key of your network.

Tx Key **Key 1** is the transmit key used by the bridge.

Authentication The default is **Auto**, which allows either Open system or Shared key authentication to be used. Select **Open** to use open system authentication; the sender and recipient do not use a WEP key for authentication. Select **Shared** to use shared key authentication; the sender and recipient use a WEP key for authentication.

Click **Refresh** to update the on-screen information.

After you have entered the security settings, click **Connect**.

Wireless > WMM®

Configure the Wireless MultiMedia (WMM) settings. WMM prioritizes packets depending on their respective access mode (traffic type): Background, Best Effort, Video, or Voice. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.



NOTE
The settings on the *WMM* screen are designed for advanced users only.

WMM

Access Mode

You can assign different settings to the four access modes available. Select the mode you want to configure: **Background**, **Best Effort**, **Video**, or **Voice**. Follow the instructions for the mode you select.

Background

Use Aggregation This option defines whether or not the Media Access Control (MAC) layer will set up an Add Block Acknowledgement (ADDBA) session. The default is **No**. Select **Yes** to enable this option.

Accept Aggregation This option defines whether or not the MAC layer will accept an ADDBA request. The default is **Yes**. Select **No** to disable this option.

Max. Number of Packets in Aggregation This option defines the maximum number of packets (sub-frames) in the aggregate. The range is **0** to **7**. The default is **7**.

Max. Aggregation Size This option defines the maximum size of the aggregate (in bytes). The range is **0** to **16000**. The default is **12000**.

Timeout Internal This option defines the timeout period in which the aggregate should be closed with a "closing condition" before it is closed by the timer. The range is **0** to **100** ms. The default is **3**.

Min. Size of Packet in Aggregation This option defines the minimum size (in bytes) of packets to be accumulated in the aggregate. The range is **0** to **1500**. The default is **10**.

ADDBA Timeout This option defines the duration after which the ADDBA setup is terminated, if there are no frame exchanges within this duration by the Block Acknowledgement (ACK) agreement. The range is **0** to **65535** ms. The default is **0**, which disables the timeout.

Aggregation Window Size This option defines the maximum number of packets transmitted without getting ACKs. The range is **0** to **64**. The default is **64**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Best Effort

Use Aggregation This option defines whether or not the Media Access Control (MAC) layer will set up an Add Block Acknowledgement (ADDBA) session. The default is **Yes**. Select **No** to disable this option.

Accept Aggregation This option defines whether or not the MAC layer will accept an ADDBA request. The default is **Yes**. Select **No** to disable this option.

Max. Number of Packets in Aggregation This option defines the maximum number of packets (sub-frames) in the aggregate. The range is **0** to **10**. The default is **10**.

Max. Aggregation Size This option defines the maximum size of the aggregate (in bytes). The range is **0** to **20000**. The default is **16000**.

Timeout Internal This option defines the timeout period in which the aggregate should be closed with a "closing condition" before it is closed by the timer. The range is **0** to **100** ms. The default is **3**.

Min. Size of Packet in Aggregation This option defines the minimum size (in bytes) of packets to be accumulated in the aggregate. The range is **0** to **1500**. The default is **10**.

ADDBA Timeout This option defines the duration after which the ADDBA setup is terminated, if there are no frame exchanges within this duration by the Block Acknowledgement (ACK) agreement. The range is **0** to **65535** ms. The default is **0**, which disables the timeout.

Aggregation Window Size This option defines the maximum number of packets transmitted without getting ACKs. The range is **0** to **64**. The default is **64**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Video

Use Aggregation This option defines whether or not the Media Access Control (MAC) layer will set up an Add Block Acknowledgement (ADDBA) session. The default is **Yes**. Select **No** to disable this option.

Accept Aggregation This option defines whether or not the MAC layer will accept an ADDBA request. The default is **Yes**. Select **No** to disable this option.

Max. Number of Packets in Aggregation This option defines the maximum number of packets (sub-frames) in the aggregate. The range is **0** to **7**. The default is **7**.

Max. Aggregation Size This option defines the maximum size of the aggregate (in bytes). The range is **0** to **16000**. The default is **12000**.

Timeout Internal This option defines the timeout period in which the aggregate should be closed with a "closing condition" before it is closed by the timer. The range is **0** to **100** ms. The default is **3**.

Min. Size of Packet in Aggregation This option defines the minimum size (in bytes) of packets to be accumulated in the aggregate. The range is **0** to **1500**. The default is **10**.

ADDBA Timeout This option defines the duration after which the ADDBA setup is terminated, if there are no frame exchanges within this duration by the Block Acknowledgement (ACK) agreement. The range is **0** to **65535** ms. The default is **0**, which disables the timeout.

Aggregation Window Size This option defines the maximum number of packets transmitted without getting ACKs. The range is **0** to **64**. The default is **64**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Voice

Use Aggregation This option defines whether or not the Media Access Control (MAC) layer will set up an Add Block Acknowledgement (ADDBA) session. The default is **Yes**. Select **No** to disable this option.

Accept Aggregation This option defines whether or not the MAC layer will accept an ADDBA request. The default is **Yes**. Select **No** to disable this option.

Max. Number of Packets in Aggregation This option defines the maximum number of packets (sub-frames) in the aggregate. The range is **0** to **2**. The default is **2**.

Max. Aggregation Size This option defines the maximum size of the aggregate (in bytes). The range is **0** to **16000**. The default is **10000**.

Timeout Internal This option defines the timeout period in which the aggregate should be closed with a "closing condition" before it is closed by the timer. The range is **0** to **100** ms. The default is **10**.

Min. Size of Packet in Aggregation This option defines the minimum size (in bytes) of packets to be accumulated in the aggregate. The range is **0** to **1500**. The default is **10**.

ADDBA Timeout This option defines the duration after which the ADDBA setup is terminated, if there are no frame exchanges within this duration by the Block Acknowledgement (ACK) agreement. The range is **0** to **65535** ms. The default is **0**, which disables the timeout.

Aggregation Window Size This option defines the maximum number of packets transmitted without getting ACKs. The range is **0** to **64**. The default is **64**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Advanced Wireless Settings

Configure the bridge's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.



NOTE
The settings on the *Advanced Wireless Settings* screen are designed for advanced users only.

Advanced Wireless

Use LDPC Low-Density Parity-Check Code (LDPC) enables or disables error correction to reduce the probability of data loss in noisy channels. The Rate Adaptation algorithm automatically disabled LDPC coding when working at high PHY rates (higher than 162). To use the LDCP advanced error correction scheme, keep the default, **Yes**. Otherwise, select **No**.

ERP Protection Type This option configures protection of OFDM packets despite the presence of 802.11b stations within the wireless network. By sending RTS/CTS or CTS2Self packets in 802.11b rates, the bridge informs the wireless network that OFDM packets are going to be transferred and protects the packets in the wireless network. The RTS/CTS and CTS2Self packets create overhead, which may result in lower throughputs.

The RTS/CTS option provides better coverage but lower throughputs when compared to CTS2Self, because the RTS/CTS option includes acknowledgement from the receiving device. To use the RTS/CTS option, keep the default, **RTS/CTS**. The None option may cause collisions between OFDM and CCK packets. To use the None option, select **None**. To use the CTS2Self option, select **CTS2Self**.

11n Protection Type This option configures protection from non-High Throughput (HT) devices within the wireless network. In case the wireless router (or access point) detects an association of a non-HT legacy device, it will signal all the HT devices to use RTS/CTS or CTS2Self mechanisms before each data transmission. This feature also supports all 802.11n standard protections, including MIMO.

The RTS/CTS option provides better coverage but lower throughputs when compared to CTS2Self, because the RTS/CTS option includes acknowledgement from the receiving device. To use the RTS/CTS option, keep the default, **RTS/CTS**. The None option may cause collisions between HT and legacy packets. To use the None option, select **None**. To use the CTS2Self option, select **CTS2Self**.

Percentage of maximal transmit power This option sets the percentage of maximal transmit power relative to the regulatory domain restrictions. For example, if the regulatory domain restriction allows transmissions of up to 20 dB, then setting the percentage at 50% allows maximal transmit power of 10 dB. Select the percentage you want to use: **12%**, **25%**, **50%**, or **100%**. The default is **100%**.

QoS Classification Type This option sets 802.1D or 802.1Q mapping from the IP DSCP/TOS field to WMM priorities (Background, Best Effects, Video, Voice). Keep the default, **802.1D**, or select **802.1Q**, which is used by some IPTV streams.

Re-establish Ethernet connection when initiating wireless connection To trigger DHCP discovery from the device that resides behind the bridge, the bridge will reset the Ethernet link between the bridge and the device every time a wireless connection is established. To disable this behavior, select **No**. Otherwise, keep the default, **Yes**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Administration > Management

Use this screen to manage specific bridge functions: access to the web-based utility, backup of the configuration file, and reboot.



Management

Bridge Access

Use a password to protect access to the browser-based utility.

Bridge Password Enter a new Password for the bridge.

Re-enter to confirm Enter the Password again to confirm.

Idle Timeout The login times out after a period of inactivity that you specify. The range is **60** to **3600** seconds. The default is **600**.

Web Access

Access via Wireless If you are using the bridge in a public domain where you are giving wireless access to your guests, you can disable wireless access to the bridge's browser-based utility. You will only be able to access the browser-based utility via a wired connection if you disable the setting. Keep the default, **Enabled**, to allow wireless access to the bridge's browser-based utility, or select **Disabled** to block wireless access to the utility.

Backup and Restore

Backup To back up the bridge's configuration file, click **Backup Configurations**. Then follow the on-screen instructions.

Restore Click **Browse** and select the configuration file. Then click **Restore Configurations**.

System Reboot

Reboot To reboot or restart the bridge, click **Start to Reboot**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Administration > Factory Defaults

Use this screen to restore the bridge's configuration to its factory default settings.

Factory Defaults

Restore All Settings To reset the bridge's settings to the factory defaults, click **Restore All Settings**. Any settings you have saved will be lost when the default settings are restored.



Administration > Upgrade Firmware

Use this screen to upgrade the bridge's firmware. Do not upgrade the firmware unless you are experiencing problems with the bridge or the new firmware has a feature you want to use.



Before upgrading the firmware, download the bridge's firmware upgrade file from the Linksys website, **www.Linksys.com/support**.

Upgrade Firmware

Please select a file to upgrade the firmware Click **Browse** and select the firmware upgrade file. Then click **Start to Upgrade** and follow the on-screen instructions.

Status > Bridge

The bridge's current status information is displayed.



Bridge Information

Firmware Version The bridge's current firmware is displayed.

Local Network

Local MAC Address The bridge's MAC Address, as seen on your local, Ethernet network, is displayed.

IP Address The bridge's IP Address, as seen on your local, Ethernet network, is displayed.

Subnet Mask The Subnet Mask configured for your local network is displayed.

Status > Wireless

Information about your wireless network is displayed.



Wireless

Link Status The status of the connection to your wireless network is displayed.

MAC Address The bridge's MAC Address, as seen on your local, wireless network, is displayed.

Network Name (SSID) The wireless network name or SSID is displayed.

BSSID The wireless MAC address of the connected wireless router (or access point) is displayed.

Radio Band The radio band of your wireless network is displayed.

Channel Width The channel width, in MHz, used by your wireless network is displayed.

Wide Channel Depending on the channel settings of your network router, the Wide Channel is displayed. If you selected Wide - 40MHz Channel for the router's Radio Band or Channel Width setting, then this will be your primary Wireless-N channel.

Standard Channel The Standard Channel setting is displayed. If you selected Wide – 40MHz Channel for the router's Radio Band or Channel Width setting, then the Standard Channel will be a secondary channel for Wireless-N.

Bit Rate The data transmission rate is displayed.

Signal The percentage of signal strength is displayed. 100% is the strongest signal strength possible; 0% is the weakest possible.

Security The security method of your wireless network is displayed.

Troubleshooting

WES610N/WET610N

Your computer or other wired, Ethernet device cannot communicate with the wireless router.

1. Access the bridge's browser-based utility.
2. On the *Basic Wireless Settings* screen, make sure the Network Name (SSID) matches the name of your wireless network.
3. Make sure the security settings (WPA, WPA2, or WEP) match the security settings of your wireless network.

The bridge's IP address needs to be changed.

If the bridge is connected to a network with a DHCP server (usually the network router), then the bridge will obtain its IP address from the DHCP server. If there is no DHCP server, then the bridge will use its default, static IP address, **169.254.1.250**.

If you want the bridge to always use a static IP address, then follow these instructions:

1. Access the bridge's browser-based utility.
2. Click the **Network Setup** tab.
3. From the *Network Connection Type* drop-down menu, select **Static IP**.
4. Complete the *Static IP Address*, *Subnet Mask*, and *Default Gateway* fields.
5. Click **Save Settings**.

The bridge-enabled computer or other wired, Ethernet device will not communicate with another wireless-enabled device (such as a computer or printer).

Check the following:

- Make sure the wireless-enabled device is on the same wireless network as the computer or other wired, Ethernet device connected to the bridge.
- Make sure that the same Network Name (SSID) is used for all devices on the wireless network.
- Make sure all devices are on the same IP network, using compatible IP addresses.

The browser-based utility does not accept your password.

Check the following:

- The password is case-sensitive. Make sure that you are using the correct case(s) when entering the password.
- If you forget your password, you can reset the bridge to its factory defaults.

 Press and hold the bridge's **Reset** button for approximately five seconds; the password will be reset to its factory default, **admin**. All other bridge settings will be reset to the factory defaults as well. (To access the browser-based utility, enter **admin** in the *Password* field.)

After you make changes through the browser-based utility, the new settings are not displayed on-screen.

On your web browser, click **Refresh**. If the new settings are not displayed, then follow these instructions:

1. Unplug the power adapter from the bridge.
2. Wait five seconds, and then plug the power adapter back into the bridge.
3. On your web browser, click **Refresh**.

WEB
If your questions are not addressed here, refer to the Linksys website at **Linksys.com/support**

Specifications

WES610N

Model	WES610N
Standards	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LEDs	Power, Ethernet, Wi-Fi Protected Setup™, Wireless, individual Ethernet link and activity
Ports	Ethernet (4), Power
Buttons	Reset, Wi-Fi Protected Setup
Cabling Type	CAT5e
Antennas	3 (internal)
Antenna Connector Type	N/A
Detachable (Yes/No)	No
Modulations	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	802.11a: 15 dBm (typical) @ 54Mbps 802.11b: 19 dBm (typical) @ 11 Mbps 802.11g: 16 dBm (typical) @ 54 Mbps 802.11n (2.4 GHz): 18 dBm (typical) @ MCS15 802.11n (5 GHz): 16 dBm (typical) @ MCS15
Receive Sensitivity	802.11a: -72 dBm (typical) @ 54 Mbps 802.11b: -85 dBm (typical) @ 11 Mbps 802.11g: -73 dBm (typical) @ 54 Mbps 802.11n (20 MHz): -75 dBm (typical) @ MCS15 802.11n (40 MHz): -69 dBm (typical) @ MCS15
Antenna Gain in dBi	1
Wireless Security	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Security Key Bits	Up to 128-bit encryption

Environmental

Dimensions	6.97" x 5.04" x 2.68" (177 x 128 x 68 mm)
Weight	0.65 lb (295 g)
Certification	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Power	12V, 1A
Operating Temperature	32 to 104ºF (0 to 40ºC)
Storage Temperature	-4 to 140ºF (-20 to 60ºC)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Specifications are subject to change without notice.

WET610N

Model	WET610N
Standards	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LEDs	Power, Ethernet, Wi-Fi Protected Setup™, Wireless
Ports	Ethernet, Power
Buttons	Reset, Wi-Fi Protected Setup
Cabling Type	CAT5e
Antennas	3 (internal)
Antenna Connector Type	N/A
Detachable (Yes/No)	No
Modulations	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	802.11a: 15 dBm (typical) @ 54Mbps 802.11b: 18 dBm (typical) @ 11 Mbps 802.11g: 16 dBm (typical) @ 54 Mbps 802.11n: 12 dBm (typical) @ 130 Mbps (HT20), 270 Mbps (HT40)
Receive Sensitivity	802.11a: -72 dBm (typical) @ 54 Mbps 802.11b: -85 dBm (typical) @ 11 Mbps 802.11g: -73 dBm (typical) @ 54 Mbps 802.11n: -70 dBm (typical) @ MCS15/2.4 GHz, -69 dBm (typical) @ MCS15/5.0 GHz
Antenna Gain in dBi	1
Wireless Security	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Security Key Bits	Up to 128-bit encryption

Environmental

Dimensions	5.71" x 4.17" x 2.05" (145 x 106 x 52 mm)
Weight	5.61 oz (159 g)
Certification	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Power	12V, 1A
Operating Temperature	32 to 104ºF (0 to 40ºC)
Storage Temperature	-4 to 140ºF (-20 to 60ºC)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Specifications are subject to change without notice.

Linksys.com/support

Cisco, the Cisco logo, and Linksys are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and other countries.
A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. All other trademarks mentioned in this document are the property of their respective owners.

© 2011 Cisco and/or its affiliates. All rights reserved.

3425-01249



دليل المستخدم

Linksys WET610N/WES610N | جسر الترفيه N مزدوج النطاق

المحتويات

نظرة عامة على المنتج

لوحة الأضواء 2
لوحة المنافذ 3

قائمة التحقق من الأمان اللاسلكي

تغيير اسم الشبكة اللاسلكية الافتراضي أو SSID 4
تغيير كلمة المرور الافتراضية 4
تمكين تصفية عنوان MAC 4
تمكين التشفير 4
الإرشادات العامة لأمان الشبكة 4
تلميحات إضافيّة للأمان 5

التكوين المتقدّم

كيفية الوصول إلى أداة المساعدة المستندة إلى مستعرض 6
Setup (الإعداد) > Basic Setup (الإعداد الأساسي) 6
Language (اللغة) 7
Network Setup (إعداد الشبكة) 7
Wireless (اللاسلكي) > Basic Wireless Settings (الإعدادات اللاسلكية الأساسية) 7
Basic Wireless Settings (الإعدادات اللاسلكية الأساسية) 7
Wireless Security (الأمان اللاسلكي) 8
Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi) 9
Wireless (اللاسلكي) > Wireless Network Site Survey (مسح موقع الشبكة اللاسلكية) 9
Wireless Network Site Survey (مسح موقع الشبكة اللاسلكية) 10
Wireless (اللاسلكي) > WMM® 11
WMM 11
Wireless (اللاسلكي) > Advanced Wireless Settings (الإعدادات اللاسلكية المتقدّمة) 13
Advanced Wireless (الإعدادات اللاسلكية المتقدّمة) 13
Administration (الإدارة) > Management (إدارة) 14
Management (إدارة) 14
Administration (الإدارة) > Factory Defaults (الإعدادات الافتراضية للشركة المصنّعة) 14
Factory Defaults (الإعدادات الافتراضية للشركة المصنّعة) 15
Administration (الإدارة) > Upgrade Firmware (ترقية البرنامج الثابت) 15
Upgrade Firmware (ترقية البرنامج الثابت) 15
Status (الحالة) > Bridge (الجسر) 15
Bridge Information (معلومات الجسر) 15
Local Network (الشبكة المحلية) 15
Status (الحالة) > Wireless (اللاسلكي) 16
Wireless (اللاسلكي) 16

استكشاف الأخطاء وإصلاحها

WES610N/WET610N 17

المواصفات

WES610N 18
WET610N 19

نظرة عامة على المنتج

شكراً لك لاختيارك جسر الترفيه N مزدوج النطاق من Linksys. يستطيع الجسر توصيل أي جهاز Ethernet سلكي بشبكتك اللاسلكية. يعتمد الجسر على تقنية لاسلكي-N مزدوجة النطاق لذا فإنه متوافق مع أي نقطة وصول أو موجّه لاسلكي-N أو G أو A أو B. بالنسبة للتثبيت لأول مرة، اتبع الخطوات الموجودة في مجلد القرص المضغوط. لتكوين الإعدادات المتقدّمة، استخدم أداة المساعدة المستندة إلى مستعرض الملائمة.

لوحة الأضواء



WES610N WET610N

لاسلكي (أزرق) يضيء ضوء اللاسلكي عندما يكون هناك اتصال لاسلكي. يومض الضوء عندما يرسل الجسر فعلياً بيانات أو يتلقاها عبر الشبكة اللاسلكية.

زر الإعداد المحمي بتقنية Wi-Fi إذا كان الموجّه الخاص بك يعتمد الإعداد المحمي بتقنية Wi-Fi ويستخدم أمان WPA أو WPA2، فيمكنك استخدام الإعداد المحمي بتقنية Wi-Fi لتوصيل الجسر تلقائياً. لاستخدام الإعداد المحمي بتقنية Wi-Fi، راجع "Wireless (اللاسلكي) > Basic Wireless Settings (الإعدادات اللاسلكية الأساسية)" في الصفحة 7.

ضوء الإعداد المحمي بتقنية Wi-Fi (أزرق/كهرماني) يومض الضوء باللون الأزرق لمدة دقيقتين أثناء الإعداد المحمي بتقنية Wi-Fi. يضيء باللون الأزرق عندما يكون الأمان اللاسلكي ممكّناً. إذا حدث خطأ أثناء عملية الإعداد المحمي بتقنية Wi-Fi، فسيضيء الضوء باللون الكهرماني. تأكد من أن موجّه الشبكة يعتمد الإعداد المحمي بتقنية Wi-Fi. انتظر حتى ينطفئ الضوء ثم حاول مجدداً.

Ethernet (أزرق) يضيء ضوء Ethernet عندما يكون هناك اتصال سلكيّ. يومض الضوء عندما يرسل الجسر فعلياً بيانات أو يتلقاها عبر منفذ (منافذ) Ethernet.

الطاقة (أزرق) يضيء ضوء الطاقة عندما يكون الجسر قيد التشغيل.

لوحة المنافذ



WES610N WET610N

Ethernet يقوم منفذ (منافذ) Ethernet بتوصيل الجسر بكمبيوتر أو جهاز شبكة Ethernet آخر. يحتوي WES610N على أربعة منافذ بينما يحتوي WET610N على منفذ واحد.

إعادة التعيين هناك طريقتان لإعادة تعيين الإعدادات الافتراضية للشركة المصنّعة الخاصة بالجسر. يمكنك إما الضغط باستمرار على زر إعادة التعيين لمدة خمس ثوان تقريباً، أو استعادة الإعدادات الافتراضية من Administration (الإدارة) > Factory Defaults (الإعدادات الافتراضية للشركة المصنّعة) في أداة المساعدة المستندة إلى مستعرض الخاصة بالجسر. في WES610N، يوجد زر إعادة التعيين على الجزء السفلي، بينما في WET610N، يوجد زر إعادة التعيين على لوحة المنافذ الخلفية.

الطاقة يعمل منفذ الطاقة على توصيل الجسر بمحوّل الطاقة المضمّن.

قائمة التحقق من الأمان اللاسلكي

إن الشبكات اللاسلكية ملائمة وسهلة التثبيت لذلك يتم التهافت إلى اعتمادها في المنازل المزوّدة بوصول عالي السرعة إلى إنترنت. وبما أن الشبكات اللاسلكية تعمل وفقاً لمبدأ إرسال المعلومات عبر موجات الراديو، لذلك هي عرضة لهجمات المتطفلين أكثر من الشبكات السلكية التقليدية. إن الإشارات الصادرة من شبكتك اللاسلكية عرضة للتعقّب شأنها شأن إشارات هاتفك الخلوي أو اللاسلكي. وبما أنه يتعذّر عليك أن تمنع أحداً فعلياً من الاتصال بشبكتك اللاسلكية، عليك اتخاذ بعض الخطوات الإضافيّة للإبقاء على شبكتك آمنة.

تغيير اسم الشبكة اللاسلكية الافتراضي أو SSID

للأجهزة اللاسلكية اسم شبكة لاسلكية افتراضي أو معرّف مجموعة خدمات (SSID) يتم تعيينه من قبل الشركة المصنّعة. هذا هو اسم شبكتك اللاسلكية ويمكن أن يتألف طوله من 32 حرفاً كحد أقصى. تستخدم منتجات Linksys اللاسلكية كلمة **linksys** كاسم الشبكة اللاسلكية الافتراضي. عليك تغيير اسم الشبكة اللاسلكية واختيار اسم فريد لتمييز شبكتك اللاسلكية عن الشبكات اللاسلكية الأخرى التي قد تحيط بك، ولكن لا تقم باستخدام معلومات شخصية (كرقم ضمانك الاجتماعي مثلاً) لأن مثل هذه المعلومات قد تكون رؤيتها متاحة لأي شخص عند استعراض الشبكات اللاسلكية.

تغيير كلمة المرور الافتراضية

بالنسبة للمنتجات اللاسلكية كنقاط الوصول والموجّات، سيُطلب منك إدخال كلمة مرور عندما تريد تغيير إعداداتها. ولهذه الأجهزة كلمة مرور افتراضية تعيّنها الشركة المصنّعة. إن كلمة المرور الافتراضية التي تعتمدها Linksys هي **admin**. يكون المتطفلون على علم بهذه الإعدادات الافتراضية وقد يحاولون استخدامها للوصول إلى جهازك اللاسلكي وتغيير إعدادات شبكتك. لإحباط أي تغييرات غير مخوّلة، قم بتخصيص كلمة المرور الخاصة بجهازك بحيث يصعب تخمينها.

تمكين تصفية عنوان MAC

تتيح لك موجّهات Linksys تمكين تصفية عنوان التحكم بالوصول إلى الوسائط (MAC). إن عنوان MAC عبارة عن سلسلة فريدة من الأرقام والأحرف يتم تعيينها لكل جهاز متّصل بالشبكة. ومع تمكين تصفية عنوان MAC، سيتم توفير الوصول إلى الشبكة اللاسلكية للأجهزة اللاسلكية التي لها عناوين MAC محددة فقط. على سبيل المثال، يمكنك تحديد عنوان MAC لكل كمبيوتر في منزلك فيكون بإمكان أجهزة الكمبيوتر هذه فقط الوصول إلى شبكتك اللاسلكية.

تمكين التشفير

يحمي التشفير البيانات التي يتم إرسالها عبر الشبكة اللاسلكية. يوفر الوصول المحمي بتقنية Wi-Fi (WPA/WPA2) والخصوصية المضاهية للسلكية (WEP) مستويات مختلفة من الأمان للاتصال اللاسلكي.

تكون الشبكة المشفّرة بواسطة WPA/WPA2 أكثر أماناً من الشبكة المشفرة بواسطة WEP لأن WPA/WPA2 يستخدم تشفير مفاتيح حيوياً لحماية المعلومات عند عبورها الموجات الهوائية. عليك تمكين أعلى مستوى من التشفير الذي يعتمده جهازك المتّصل بالشبكة.

إن WEP هو معيار تشفير قديم وقد يكون الخيار الوحيد المتوفر على بعض الأجهزة القديمة التي لا تعتمد WPA.

الإرشادات العامة لأمان الشبكة

لا فائدة من أمان الشبكة اللاسلكية إذا ما كانت الشبكة الأساسية غير آمنة.

- تحمي كلمة المرور كافة أجهزة الكمبيوتر على الشبكة في حين تحمي كلمة المرور الفردية الملفات الحساسة.
- قم بتغيير كلمات المرور بانتظام.
- قم بتثبيت برنامج الحماية من الفيروسات وبرنامج جدار الحماية الشخصي.
- قم بتعطيل مشاركة الملفات (نظير إلى نظير). قد تفتح بعض التطبيقات مشاركة الملفات من دون موافقتك و/أو معرفتك.

تلميحات إضافيّة للأمان

- قم بإبقاء الموجّهات أو نقاط الوصول أو العبّارات اللاسلكية بعيدة عن الجدران الخارجية والنوافذ.
- قم بإيقاف تشغيل الموجّهات أو نقاط الوصول أو العبّارات اللاسلكية أثناء عدم استخدامها (أثناء الليل، خلال أيام العطل).
- استخدم جمل مرور قويّة يتألّف طولها من ثمانية أحرف على الأقلّ. قم بدمج الأحرف والأرقام لتفادي استخدام الكلمات القياسية التي يمكن العثور عليها في القاموس.

التكوين المتقدّم

بعد إعداد الجسر عن طريق اتباع الخطوات الموضحة في مجلد القرص المضغوط، يكون الجسر جاهزاً للاستخدام. ولكن إن أردت تغيير إعداداته المتقدّمة، فاستخدم الأداة المساعدة المستندة إلى مستعرض الخاصة بالجسر. يصف هذا الفصل كل صفحة من صفحات ويب الخاصة بأداة المساعدة مع أبرز الوظائف الخاصة بكل صفحة. يمكنك الوصول إلى أداة المساعدة عبر مستعرض ويب على جهاز كمبيوتر متصل بالجسر.

تحتوي أداة المساعدة المستندة إلى مستعرض على علامات التبويب الأساسية التالية: Setup (الإعداد) وWireless (اللاسلكي) وAdministration (الإدارة) وStatus (الحالة). وستتوفر علامات تبويب إضافيّة بعد أن تنقر فوق إحدى علامات التبويب الرئيسيّة.

كيفية الوصول إلى أداة المساعدة المستندة إلى مستعرض

استخدم مستعرض ويب للوصول إلى أداة المساعدة المستندة إلى مستعرض.

إذا كان الجسر متصلاً بشبكة مزوّدة بخادم DHCP (عادة موجّه الشبكة)، فسيحصل الجسر على عنوان IP من خادم DHCP. في حالة عدم وجود خادم DHCP، سيستخدم الجسر عنوان IP الثابت الافتراضي الخاص به، **169.254.1.250**. (إذا قمت بتعيين عنوان IP ثابت دائم على الجسر عبر أداة المساعدة المستندة إلى مستعرض، فأدخل عنوان IP الثابت بدلاً من ذلك).

ملاحظة

إذا كنت لا تعرف عنوان IP الخاص بالجسر، فابحث عن عنوان IP الخاص به في جدول عملاء DHCP الخاص بالموجّه. (راجع وثائق الموجّه الخاص بك).

إذا لم تستطع تحديد موقع عنوان IP الخاص بالجسر، فيمكنك إعادة تعيين الجسر: اضغط على زر **إعادة التعيين** على الجسر لمدة خمس ثوانٍ تقريباً باستخدام مشبك ورق مستقيم. سيؤدي ذلك إلى إعادة تعيين الجسر إلى الإعدادات الافتراضية الخاصة بالشركة المصنّعة. سيطلب الجسر عنوان IP من خادم DHCP (عادة موجّه الشبكة). في حالة عدم العثور على خادم DHCP، يستخدم الجسر عنوان IP الثابت الافتراضي الخاص به، **169.254.1.250**، حتى يكتشف خادم DHCP ويتم تعيين عنوان IP حيوي للجسر.

إذا كان الجسر غير مقترن بموجّه وكان يستخدم الإعدادات الافتراضية للشركة المصنّعة، فقم بتوصيل الكمبيوتر بالجسر باستخدام اتصال Ethernet للوصول إلى أداة المساعدة المستندة إلى ويب. ستحتاج إلى تكوين اتصال Ethernet على الكمبيوتر باستخدام عنوان IP ثابت وقناع شبكة فرعية.

يجب تعيين عنوان IP الخاص بمحوّل Ethernet على عنوان IP محدد.

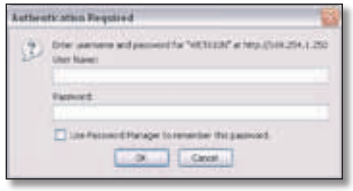
1. في حقل *IP address (عنوان IP)*، أدخل **169.254.x.y** (يجب استبدال x برقم بين 1 و254 وy برقم بين 0 و255).
2. في حقل *Subnet mask (قناع الشبكة الفرعية)*، أدخل **255.255.0.0**.

ملاحظة

تختلف خطوات تعيين عنوان IP ثابت لمحوّل Ethernet على الكمبيوتر الخاص بك تبعاً لنظام التشغيل. للاطلاع على التعليمات، الرجاء مراجعة وثائق التعليمات لنظام التشغيل الخاص بك.

بعد تعيين عنوان IP ثابت لمحوّل Ethernet، قم بتشغيل مستعرض ويب وأدخل عنوان IP الخاص بالمحوّل (الإعداد الافتراضي **169.254.1.250**) في حقل *Address (العنوان)*. اضغط على **Enter (إدخال)**.

تظهر شاشة طلب كلمة المرور. (سيرى المستخدمون الذين لا يعتمدون أنظمة Windows XP شاشة مشابهة). اترك حقل *User name (اسم المستخدم)* فارغاً. أدخل كلمة المرور التي أنشأتها أثناء معالج الإعداد. إذا لم تكن قد أنشأت كلمة مرور جديدة، فاستخدم كلمة المرور الافتراضية، **admin**. (يمكنك تعيين كلمة مرور جديدة من الشاشة *Administration (الإدارة) > Management (إدارة)*). انقر فوق **OK (موافق)** للمتابعة.



ملاحظة

إذا لم تظهر شاشة طلب كلمة المرور، فانتظر دقيقتين وحاول مرة أخرى.

Setup (الإعداد) > Basic Setup (الإعداد الأساسي)

أول شاشة تظهر هي شاشة *Basic Setup (الإعداد الأساسي)*. استخدم هذه الشاشة لتغيير لغة أداة المساعدة المستندة إلى مستعرض أو لتغيير إعدادات شبكة Ethernet السلكية الخاصة بالجسر.





Language (اللغة)

Language (اللغة) تُستخدم لتعيين اللغة المعروضة بواسطة أداة المساعدة المستندة إلى مستعرض. حدد اللغة المطلوبة من القائمة المنسدلة.

Network Setup (إعداد الشبكة)

يحدد هذا القسم ما إذا تم الحصول على عنوان IP الخاص بالجسر تلقائياً من خادم DHCP مثل موجّه الشبكة (Automatic Configuration - DHCP (تكوين تلقائي - DHCP)) أو تم تعيينه يدوياً (Static IP (IP ثابت)).

Bridge IP (IP الجسر) إذا كانت شبكتك مزودة بخادم DHCP، مثل موجّه الشبكة، يقوم بتعيين عناوين IP لأجهزة الشبكة الخاصة بك. فأبقِ على الإعداد الافتراضي **Automatic Configuration - DHCP (تكوين تلقائي - DHCP)**. سيطلب الجسر عنوان IP من خادم DHCP (عادة موجّه الشبكة). في حالة عدم العثور على خادم DHCP، يستخدم الجسر عنوان IP الثابت الافتراضي الخاص به، **169.254.1.250**، حتى يكتشف خادم DHCP ويتم تعيين عنوان IP حيوي للجسر.

إذا أردت تعيين عنوان IP ثابت دائم للجسر، فحدد **Static IP (IP ثابت)**.

إذا حددت Static IP (IP ثابت)، فأكمل الحقول التالية:

- **Static IP Address (عنوان IP ثابت)** أدخل عنوان IP فريداً سيتم استخدامه للوصول إلى أداة المساعدة المستندة إلى مستعرض.
- **Subnet Mask (قناع الشبكة الفرعية)** أدخل قناع الشبكة الفرعية الخاص بالشبكة السلكية.
- **Default Gateway (العبّارة الافتراضية)** أدخل عنوان IP للعبّارة الافتراضية الخاصة بشبكتك (في معظم الحالات، يكون الموجّه الخاص بك).

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Wireless (اللاسلكي) > Basic Wireless Settings (الإعدادات اللاسلكية الأساسية)

استخدم شاشة *Basic Wireless Settings (الإعدادات اللاسلكية الأساسية)* لتكوين الإعدادات اللاسلكية الأساسية وإعدادات الأمان الخاصة بالجسر.

هناك طريقتان لتكوين إعدادات الجسر، هما manual (يدوي) وWi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi). والإعداد المحمي بتقنية Wi-Fi هو ميزة تعمل على تسهيل إعداد شبكتك اللاسلكية. إذا كان موجّه الشبكة الخاص بك يعتمد الإعداد المحمي بتقنية Wi-Fi ويستخدم أمان WPA أو WPA2، فيمكنك استخدام الإعداد المحمي بتقنية Wi-Fi لتوصيل الجسر تلقائياً.

Configuration View (عرض التكوين) لتكوين شبكتك اللاسلكية يدوياً، حدد **Manual (يدوي)**. راجع **Basic Wireless Settings (الإعدادات اللاسلكية الأساسية)**، **صفحة 8**. لاستخدام الإعداد المحمي بتقنية Wi-Fi، حدد **Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)**. راجع **Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)**، **صفحة 9**.

Basic Wireless Settings (الإعدادات اللاسلكية الأساسية)



Network Name (SSID) (اسم الشبكة (SSID)) SSID هو اسم الشبكة المشترك بين كافة النقاط في شبكة لاسلكية. يجب أن يكون SSID مطابقاً لكافة الأجهزة في الشبكة اللاسلكية. وهو متحسّس لحالة الأحرف ويجب ألا يزيد عن 32 حرفاً (استخدم أي أحرف موجودة على لوحة المفاتيح). تأكد من أن هذا الإعداد مطابق للإعداد الموجود على الموجّه اللاسلكي أو نقطة الوصول لديك. لمزيد من الأمان، يجب تغيير SSID الافتراضي (**linksys**) إلى اسم فريد.

Wireless Security (الأمان اللاسلكي)

يعتمد الجسر خيارات الأمان اللاسلكي التالية: WPA Personal (WPA شخصي) وWPA2 Personal (WPA2 شخصي) وWEP. WPA (الوصول المحمي بتقنية Wi-Fi) وWPA2 أسلوبا أمان أقوى من WEP (الخصوصية المضاهية للسلكية). للحصول على مزيد من المعلومات حول الأمان اللاسلكي، راجع "قائمة التحقق من الأمان اللاسلكي"، الصفحة 4.

Security Mode (وضع الأمان)

حدد أسلوب الأمان لشبكتك اللاسلكية. إذا كنت لا تريد استخدام الأمان اللاسلكي، فأبقِ على الإعداد الافتراضي **Disabled (معطّل)**.

ملاحظة
تذكر أنه يجب أن يستخدم كل جهاز في شبكتك اللاسلكية نفس أسلوب الأمان وجملة المرور/المفتاح وإلا فلن تستطيع الأجهزة اللاسلكية الاتصال ببعضها البعض.

WPA Personal (WPA شخصي)

WPA هو معيار أمان أقوى من تشفير WEP.



Encryption (التشفير) يعتمد WPA أسلوب التشفير TKIP، باستخدام مفاتيح تشفير حيوية.

Passphrase (جملة المرور) أدخل المفتاح المشترك بين الجسر والموجّه اللاسلكي أو نقطة الوصول. يجب أن تتضمن بين 8 و 63 حرفاً.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

WPA2 Personal (WPA2 شخصي)

WPA2 هو إصدار من WPA أكثر تقدماً وأماناً.



Encryption (التشفير) يعتمد WPA2 أسلوبي التشفير، TKIP وAES، باستخدام مفاتيح تشفير حيوية. حدد أسلوب التشفير، **AES** أو **TKIP or AES (TKIP أو AES)**. التحديد الافتراضي هو **AES**.

Passphrase (جملة المرور) أدخل المفتاح المشترك بين الجسر والموجّه اللاسلكي أو نقطة الوصول. يجب أن تتضمن بين 8 و 63 حرفاً.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

WEP

WEP هو أسلوب تشفير أساسي. لكنه ليس بنفس أمان WPA أو WPA2.



Encryption (التشفير) حدد مستوى تشفير WEP. **40/64 bits (10 hex digits)** (40/64 بت (10 أرقام سداسية عشرية)) أو **104/128 bits (26 hex digits)** (**104/128 بت (26 رقماً سداسياً عشرياً)**). الإعداد الافتراضي **40/64 bits (10 hex digits)** (**40/64 بت (10 أرقام سداسية عشرية)**).

Key 1 (المفتاح 1) أدخل مفتاح WEP لشبكتك.

Tx Key (مفتاح الإرسال) **Key 1 (المفتاح 1)** هو مفتاح الإرسال المستخدم بواسطة الجسر.

Authentication (المصادقة) الإعداد الافتراضي هو **Auto (تلقائي)**، والذي يسمح باستخدام مصادقة النظام المفتوح أو المفتاح المشترك. حدد **Open (مفتوح)** لاستخدام مصادقة النظام المفتوح؛ لا يستخدم المرسل والمتلقي مفتاح WEP للمصادقة. حدد **Shared (مشترك)** لاستخدام مصادقة المفتاح المشترك؛ يستخدم المرسل والمتلقي مفتاح WEP للمصادقة.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)

يتوفر أسلوبان. استخدم الأسلوب الذي ينطبق على الموجّه الذي تستخدمه.





الأسلوب 1

استخدم هذا الأسلوب إذا كان الموجّه يتضمن زر إعداد محمي بتقنية Wi-Fi.

1. انقر فوق زر **الإعداد المحمي بتقنية Wi-Fi** الموجود على الموجّه أو اضغط عليه.
2. خلال دقيقتين، انقر فوق زر **Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)** الموجود في شاشة *Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)* الخاصة بالجسر.
3. بعد تكوين الجسر، انقر فوق **Close (إغلاق)**.

تعرض شاشة *Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)* Link Status (حالة الارتباط) وNetwork Name (SSID) (اسم الشبكة (SSID)) وأسلوب Security (الأمان).

الأسلوب 2

استخدم هذا الأسلوب إذا طلب الموجّه رقم التعريف الشخصي للجسر.

1. في شاشة *Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)* الخاصة **بالموجّه**، أدخل رقم التعريف الشخصي الموجود في شاشة *Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)* الخاصة **بالجسر**. ثم انقر فوق **Register (تسجيل)** أو الزر المناسب. (رقم التعريف الشخصي مدرج أيضاً على الملصق في أسفل الجسر).
2. في شاشة *Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)* الخاصة بالجسر، انقر فوق **OK (موافق)**.
3. بعد تكوين الجسر، انقر فوق **Close (إغلاق)**.

تعرض شاشة *Wi-Fi Protected Setup (الإعداد المحمي بتقنية Wi-Fi)* Link Status (حالة الارتباط) وNetwork Name (SSID) (اسم الشبكة (SSID)) وأسلوب Security (الأمان).

Wireless (اللاسلكي) > Wireless Network Site Survey (مسح موقع الشبكة اللاسلكية)

انقر فوق علامة التبويب **Wireless Network Site Survey (مسح موقع الشبكة اللاسلكية)** لبدء مسح للموقع. تسرد شاشة *Wireless Network Site Survey (مسح موقع الشبكة اللاسلكية)* الشبكات اللاسلكية التي يكتشفها الجسر.



Wireless Network Site Survey (مسح موقع الشبكة اللاسلكية)

Number of Wireless Networks (عدد الشبكات اللاسلكية) يتم عرض عدد الشبكات اللاسلكية التي يكتشفها الجسر.

Select (تحديد) للاتصال بشبكة لاسلكية، انقر فوق **Select (تحديد)**. ثم انقر فوق **Connect (اتصال)**.

Wireless Network Name (اسم الشبكة اللاسلكية) يتم عرض اسم الشبكة أو SSID للشبكة اللاسلكية.

GHz (غيغا هرتز) يتم عرض نطاق التردد اللاسلكي للشبكة اللاسلكية.

Signal (الإشارة) يتم عرض النسبة المئوية لقوة الإشارة. 100% هي أعلى قوة إشارة ممكنة، و0% هي أضعف إشارة ممكنة.

Security (الأمان) إذا كانت الشبكة تعتمد الإعداد المحمي بتقنية Wi-Fi، فسيتم عرض رمز الإعداد المحمي بتقنية Wi-Fi . يتم عرض أسلوب الأمان المُستخدم بواسطة الشبكة اللاسلكية.

انقر فوق **Refresh (تحديث)** لتحديث المعلومات التي تظهر على الشاشة.

بعد تحديد شبكة، انقر فوق **Connect (اتصال)**. ستظهر شاشة جديدة. اتبع التعليمات الخاصة بأسلوب الأمان في شبكتك.

WPA



Network Name (SSID) (اسم الشبكة (SSID)) يتم عرض اسم الشبكة التي قمت بتحديدها تلقائياً.

Security Mode (وضع الأمان) يتم عرض WPA Personal (WPA شخصي) تلقائياً.

Encryption (التشفير) يعتمد WPA أسلوب التشفير TKIP، باستخدام مفاتيح تشفير حيوية.

Passphrase (جملة المرور) أدخل المفتاح المشترك بين الجسر والموجّه اللاسلكي أو نقطة الوصول. يجب أن تتضمن بين 8 و 63 حرفاً.

انقر فوق **Refresh (تحديث)** لتحديث المعلومات التي تظهر على الشاشة.

بعد إدخال إعدادات الأمان، انقر فوق **Connect (اتصال)**.

WPA2



Network Name (SSID) (اسم الشبكة (SSID)) يتم عرض اسم الشبكة التي قمت بتحديدها تلقائياً.

Security Mode (وضع الأمان) يتم عرض WPA2 Personal (WPA2 شخصي) تلقائياً.

Encryption (التشفير) يعتمد WPA2 أسلوبي التشفير، TKIP وAES، باستخدام مفاتيح تشفير حيوية. حدد أسلوب التشفير، **AES** أو **TKIP or AES (TKIP أو AES)**.

Passphrase (جملة المرور) أدخل المفتاح المشترك بين الجسر والموجّه اللاسلكي أو نقطة الوصول. يجب أن تتضمن بين 8 و 63 حرفاً.

انقر فوق **Refresh (تحديث)** لتحديث المعلومات التي تظهر على الشاشة.

بعد إدخال إعدادات الأمان، انقر فوق **Connect (اتصال)**.

WEP



Network Name (SSID) (اسم الشبكة (SSID)) يتم عرض اسم الشبكة التي قمت بتحديدها تلقائياً.

Security Mode (وضع الأمان) يتم عرض WEP تلقائياً.

Encryption (التشفير) حدد مستوى تشفير WEP، **40/64 bits (10 hex digits) (40/64 بت (10 أرقام سداسية عشرية))** أو **104/128 bits (26 hex digits) (104/128 بت (26 رقماً سداسياً عشرياً))**.

Key 1 (المفتاح 1) أدخل مفتاح WEP لشبكتك.

Tx Key (مفتاح الإرسال) **Key 1 (المفتاح 1)** هو مفتاح الإرسال المستخدم بواسطة الجسر.

Authentication (المصادقة) الإعداد الافتراضي هو **Auto (تلقائي)**، والذي يسمح باستخدام مصادقة النظام المفتوح أو المفتاح المشترك. حدد **Open (مفتوح)** لاستخدام مصادقة النظام المفتوح؛ لا يستخدم المرسل والمتلقي مفتاح WEP للمصادقة. حدد **Shared (مشترك)** لاستخدام مصادقة المفتاح المشترك؛ يستخدم المرسل والمتلقي مفتاح WEP للمصادقة.

انقر فوق **Refresh (تحديث)** لتحديث المعلومات التي تظهر على الشاشة.

بعد إدخال إعدادات الأمان، انقر فوق **Connect (اتصال)**.

Wireless (اللاسلكي) > WMM®

قم بتكوين إعدادات الوسائط المتعددة اللاسلكية (WMM). تقوم WMM بتحديد أولوية الحزم تبعاً لوضع الوصول الخاص بها (نوع حركة البيانات): Background (الخلفية) أو Best Effort (أفضل جهد) أو Video (فيديو) أو Voice (صوت). يجب أن يقوم مسؤول خبير فقط بضبط هذه الإعدادات إذ إنّ الإعدادات الخاطئة قد تحدّ من الأداء اللاسلكي.



ملاحظة

الإعدادات الموجودة في شاشة *WMM* مصممة للمستخدمين المتقدّمين فقط.

WMM

Access Mode (وضع الوصول)

يمكنك تعيين إعدادات مختلفة لأوضاع الوصول الأربعة المتوفرة. حدّد الوضع الذي تريد تكوينه: **Background (الخلفية)** أو **Best Effort (أفضل جهد)** أو **Video (فيديو)** أو **Voice (صوت)**. اتبع التعليمات الخاصة بالوضع الذي تحدده.

Background (الخلفية)

Use Aggregation (استخدام التجميع) يحدد هذا الخيار ما إذا كانت طبقة التحكم بالوصول إلى الوسائط (MAC) ستقوم بإعداد جلسة عمل إضافة إقرار مجمّع (ADDBA) أم لا. الإعداد الافتراضي هو **No (لا)**. حدد **Yes (نعم)** لتمكين هذا الخيار.

Accept Aggregation (قبول التجميع) يحدد هذا الخيار ما إذا كانت طبقة MAC ستقبل طلب ADDBA أم لا. الإعداد الافتراضي هو **Yes (نعم)**. حدد **No (لا)** لتعطيل هذا الخيار.

Max. Number of Packets in Aggregation (الحد الأقصى لعدد الحزم في التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم (الإطارات الفرعية) في التجميع. يتراوح النطاق ما بين **0** و **7**. الإعداد الافتراضي هو **7**.

Max. Aggregation Size (الحد الأقصى لحجم التجميع) يحدد هذا الخيار الحد الأقصى لحجم التجميع (بالبايت). يتراوح النطاق ما بين **0** و **16000**. الإعداد الافتراضي هو **12000**.

Timeout Internal (مهلة داخلية) يحدد هذا الخيار مدة المهلة التي يجب إغلاق التجميع خلالها باستخدام "شرط إغلاق" قبل أن يتم إغلاقه بواسطة المؤقت. يتراوح النطاق ما بين **0** و **100** مللي ثانية. الإعداد الافتراضي هو **3**.

Min. Size of Packet in Aggregation (الحد الأدنى لحجم الحزم في التجميع) يحدد هذا الخيار الحد الأدنى (بالبايت) لحجم الحزم التي ستتراكم في التجميع. يتراوح النطاق ما بين **0** و **1500**. الإعداد الافتراضي هو **10**.

ADDBA Timeout (مهلة ADDBA) يحدد هذا الخيار المدة التي سيتم بعدها إنهاء إعداد ADDBA في حالة عدم وجود تبادلات للإطارات خلال هذه المدة حسب اتفاقية الإقرار المجمّع (ACK). يتراوح النطاق ما بين **0** و **65535** مللي ثانية. الإعداد الافتراضي **0**. ويؤدي إلى تعطيل المهلة.

Aggregation Window Size (حجم إطار التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم التي يتم إرسالها من دون الحصول على إقرارات مجمّعة. يتراوح النطاق ما بين **0** و **64**. الإعداد الافتراضي هو **64**.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Best Effort (أفضل جهد)

Use Aggregation (استخدام التجميع) يحدد هذا الخيار ما إذا كانت طبقة التحكم بالوصول إلى الوسائط (MAC) ستقوم بإعداد جلسة عمل إضافة إقرار مجمّع (ADDBA) أم لا. الإعداد الافتراضي هو **Yes (نعم)**. حدد **No (لا)** لتعطيل هذا الخيار.

Accept Aggregation (قبول التجميع) يحدد هذا الخيار ما إذا كانت طبقة MAC ستقبل طلب ADDBA أم لا. الإعداد الافتراضي هو **Yes (نعم)**. حدد **No (لا)** لتعطيل هذا الخيار.

Max. Number of Packets in Aggregation (الحد الأقصى لعدد الحزم في التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم (الإطارات الفرعية) في التجميع. يتراوح النطاق ما بين **0** و **10**. الإعداد الافتراضي هو **10**.

Max. Aggregation Size (الحد الأقصى لحجم التجميع) يحدد هذا الخيار الحد الأقصى لحجم التجميع (بالبايت). يتراوح النطاق ما بين **0** و **20000**. الإعداد الافتراضي هو **16000**.

Timeout Internal (مهلة داخلية) يحدد هذا الخيار مدة المهلة التي يجب إغلاق التجميع خلالها باستخدام "شرط إغلاق" قبل أن يتم إغلاقه بواسطة المؤقت. يتراوح النطاق ما بين **0** و **100** مللي ثانية. الإعداد الافتراضي هو **3**.

Min. Size of Packet in Aggregation (الحد الأدنى لحجم الحزم في التجميع) يحدد هذا الخيار الحد الأدنى (بالبايت) لحجم الحزم التي ستتراكم في التجميع. يتراوح النطاق ما بين **0** و **1500**. الإعداد الافتراضي هو **10**.

ADDBA Timeout (مهلة ADDBA) يحدد هذا الخيار المدة التي سيتم بعدها إنهاء إعداد ADDBA في حالة عدم وجود تبادلات للإطارات خلال هذه المدة حسب اتفاقية الإقرار المجمّع (ACK). يتراوح النطاق ما بين **0** و **65535** مللي ثانية. الإعداد الافتراضي **0**. ويؤدي إلى تعطيل المهلة.

Aggregation Window Size (حجم إطار التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم التي يتم إرسالها من دون الحصول على إقرارات مجمّعة. يتراوح النطاق ما بين **0** و **64**. الإعداد الافتراضي هو **64**.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Video (فيديو)

Use Aggregation (استخدام التجميع) يحدد هذا الخيار ما إذا كانت طبقة التحكم بالوصول إلى الوسائط (MAC) ستقوم بإعداد جلسة عمل إضافة إقرار مجمّع (ADDBA) أم لا. الإعداد الافتراضي هو **Yes (نعم)**. حدد **No (لا)** لتعطيل هذا الخيار.

Accept Aggregation (قبول التجميع) يحدد هذا الخيار ما إذا كانت طبقة MAC ستقبل طلب ADDBA أم لا. الإعداد الافتراضي هو **Yes (نعم)**. حدد **No (لا)** لتعطيل هذا الخيار.

Max. Number of Packets in Aggregation (الحد الأقصى لعدد الحزم في التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم (الإطارات الفرعية) في التجميع. يتراوح النطاق ما بين **0** و **7**. الإعداد الافتراضي هو **7**.

Max. Aggregation Size (الحد الأقصى لحجم التجميع) يحدد هذا الخيار الحد الأقصى لحجم التجميع (بالبايت). يتراوح النطاق ما بين **0** و **16000**. الإعداد الافتراضي هو **12000**.

Timeout Internal (مهلة داخلية) يحدد هذا الخيار مدة المهلة التي يجب إغلاق التجميع خلالها باستخدام "شرط إغلاق" قبل أن يتم إغلاقه بواسطة المؤقت. يتراوح النطاق ما بين **0** و **100** مللي ثانية. الإعداد الافتراضي هو **3**.

Min. Size of Packet in Aggregation (الحد الأدنى لحجم الحزم في التجميع) يحدد هذا الخيار الحد الأدنى (بالبايت) لحجم الحزم التي ستتراكم في التجميع. يتراوح النطاق ما بين **0** و **1500**. الإعداد الافتراضي هو **10**.

ADDBA Timeout (مهلة ADDBA) يحدد هذا الخيار المدة التي سيتم بعدها إنهاء إعداد ADDBA في حالة عدم وجود تبادلات للإطارات خلال هذه المدة حسب اتفاقية الإقرار المجمّع (ACK). يتراوح النطاق ما بين **0** و **65535** مللي ثانية. الإعداد الافتراضي **0**، ويؤدي إلى تعطيل المهلة.

Aggregation Window Size (حجم إطار التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم التي يتم إرسالها من دون الحصول على إقرارات مجمّعة. يتراوح النطاق ما بين **0** و **64**. الإعداد الافتراضي هو **64**.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Voice (صوت)

Use Aggregation (استخدام التجميع) يحدد هذا الخيار ما إذا كانت طبقة التحكم بالوصول إلى الوسائط (MAC) ستقوم بإعداد جلسة عمل إضافة إقرار مجمّع (ADDBA) أم لا. الإعداد الافتراضي هو **Yes (نعم)**. حدد **No (لا)** لتعطيل هذا الخيار.

Accept Aggregation (قبول التجميع) يحدد هذا الخيار ما إذا كانت طبقة MAC ستقبل طلب ADDBA أم لا. الإعداد الافتراضي هو **Yes (نعم)**. حدد **No (لا)** لتعطيل هذا الخيار.

Max. Number of Packets in Aggregation (الحد الأقصى لعدد الحزم في التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم (الإطارات الفرعية) في التجميع. يتراوح النطاق ما بين **0** و **2**. الإعداد الافتراضي هو **2**.

Max. Aggregation Size (الحد الأقصى لحجم التجميع) يحدد هذا الخيار الحد الأقصى لحجم التجميع (بالبايت). يتراوح النطاق ما بين **0** و **16000**. الإعداد الافتراضي هو **10000**.

Timeout Internal (مهلة داخلية) يحدد هذا الخيار مدة المهلة التي يجب إغلاق التجميع خلالها باستخدام "شرط إغلاق" قبل أن يتم إغلاقه بواسطة المؤقت. يتراوح النطاق ما بين **0** و **100** مللي ثانية. الإعداد الافتراضي هو **10**.

Min. Size of Packet in Aggregation (الحد الأدنى لحجم الحزم في التجميع) يحدد هذا الخيار الحد الأدنى (بالبايت) لحجم الحزم التي ستتراكم في التجميع. يتراوح النطاق ما بين **0** و **1500**. الإعداد الافتراضي هو **10**.

ADDBA Timeout (مهلة ADDBA) يحدد هذا الخيار المدة التي سيتم بعدها إنهاء إعداد ADDBA في حالة عدم وجود تبادلات للإطارات خلال هذه المدة حسب اتفاقية الإقرار المجمّع (ACK). يتراوح النطاق ما بين **0** و **65535** مللي ثانية. الإعداد الافتراضي **0**، ويؤدي إلى تعطيل المهلة.

Aggregation Window Size (حجم إطار التجميع) يحدد هذا الخيار الحد الأقصى لعدد الحزم التي يتم إرسالها من دون الحصول على إقرارات مجمّعة. يتراوح النطاق ما بين **0** و **64**. الإعداد الافتراضي هو **64**.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Wireless (اللاسلكي) > Advanced Wireless Settings (الإعدادات اللاسلكية المتقدّمة)

قم بتكوين الوظائف اللاسلكية المتقدّمة الخاصة بالجسر. يجب أن يقوم مسؤول خبير فقط بضبط هذه الإعدادات إذ إنّ الإعدادات الخاطئة قد تحدّ من الأداء اللاسلكي.



ملاحظة

الإعدادات الموجودة في شاشة Advanced Wireless Settings (الإعدادات اللاسلكية المتقدّمة) مصممة للمستخدمين المتقدّمين فقط.

Advanced Wireless (الإعدادات اللاسلكية المتقدّمة)

Use LDPC (استخدام LDPC) يعمل رمز تدقيق التماثل منخفض الكثافة (LDPC) على تمكين أو تعطيل تصحيح الأخطاء لتقليل احتمالية فقد البيانات في القنوات المليئة بالضوضاء. تعمل خوارزمية ملاءمة المعدّل على تعطيل ترميز LDPC تلقائياً عند العمل بمعدلات PHY مرتفعة (أعلى من 162). لاستخدام نظام تصحيح الأخطاء المتقدّم الخاص بـ LDCP، أبقِ على الإعداد الافتراضي، **Yes (نعم)**. وإلا فحدد **No (لا)**.

ERP Protection Type (نوع حماية ERP) يعمل هذا الخيار على تكوين حماية حزم OFDM بالرغم من وجود محطات 802.11b داخل الشبكة اللاسلكية. عند إرسال حزم RTS/CTS أو CTS2Self بمعدلات 802.11b، يعلِم الجسرُ الشبكة اللاسلكية أنه سيتم نقل حزم OFDM ويقوم بحماية الحزم في الشبكة اللاسلكية. تؤدي حزم RTS/CTS وCTS2Self إلى إنشاء حمل زائد مما قد ينجم عنه انخفاض في حركة البيانات.

يوفر خيار RTS/CTS تغطية أفضل لكن حركة بيانات أقل مقارنة بـ CTS2Self، لأن خيار RTS/CTS يتضمن إقراراً من الجهاز المتلقي. لاستخدام خيارRTS/CTS، أبقِ على الإعداد الافتراضي، **RTS/CTS**. قد يؤدي الخيار None (بلا) إلى تضاربات بين حزم OFDM وCCK. لاستخدام الخيار None (بلا)، حدد **None (بلا)**. لاستخدام الخيار CTS2Self، حدد **CTS2Self**.

11n Protection Type (نوع حماية 11n) يعمل هذا الخيار على تكوين الحماية من أجهزة ذات حركة بيانات غير مرتفعة داخل الشبكة اللاسلكية. إذا اكتشف الموجّه اللاسلكي (أو نقطة الوصول) اقتران جهاز قديم ذي حركة بيانات غير مرتفعة، فسيرسل إشارة إلى كافة الأجهزة ذات حركة البيانات المرتفعة باستخدام آليات RTS/CTS أو CTS2Self قبل كل عملية إرسال للبيانات. كما تعتمد هذه الميزة كافة عمليات حماية 802.11n القياسية بما في ذلك MIMO.

يوفر خيار RTS/CTS تغطية أفضل لكن حركة بيانات أقل مقارنة بـ CTS2Self، لأن خيار RTS/CTS يتضمن إقراراً من الجهاز المتلقي. لاستخدام خيارRTS/CTS، أبقِ على الإعداد الافتراضي، **RTS/CTS**. قد يؤدي الخيار None (بلا) إلى تضاربات بين الحزم القديمة والحزم ذات حركة البيانات المرتفعة. لاستخدام الخيار None (بلا)، حدد **None (بلا)**. لاستخدام الخيار CTS2Self، حدد **CTS2Self**.

Percentage of maximal transmit power (النسبة المئوية لأقصى قوة إرسال) يقوم هذا الخيار بتعيين النسبة المئوية لأقصى قوة إرسال بالنسبة لقيود النطاق التنظيمية. على سبيل المثال، إذا سمح قيد النطاق التنظيمي بعمليات إرسال تصل إلى 20 ديسيبل، فإن تعيين النسبة المئوية على 50% يسمح بأن تصل أقصى قوة إرسال إلى 10 ديسيبل. حدّد النسبة المئوية التي تريد استخدامها: **12%** أو **25%** أو **50%** أو **100%**. الإعداد الافتراضي هو **100%**.

QoS Classification Type (نوع تصنيف جودة الخدمة) يعيّن هذا الخيار تعيين 802.1D أو 802.1Q من حقل IP DSCP/TOS على أولويات WMM (Background (الخلفية)، Best Effects (أفضل تأثيرات)، Video (فيديو)، Voice (صوت)). أبقِ على الإعداد الافتراضي، **802.1D**، أو حدد **802.1Q**، الذي يُستخدم بواسطة بعض تدفقات IPTV.

Re-establish Ethernet connection when initiating wireless connection (إعادة إنشاء اتصال Ethernet عند بدء اتصال لاسلكي) لتشغيل اكتشاف DHCP من جهاز يوجد خلف الجسر، يقوم الجسر بإعادة تعيين ارتباط Ethernet بين الجسر والجهاز في كل مرة يتم فيها إنشاء اتصال لاسلكي. لتعطيل هذه الوظيفة، حدد **No (لا)**. وإلا فأبقِ على الإعداد الافتراضي، **Yes (نعم)**.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Administration (الإدارة) > Management (إدارة)

استخدم هذه الشاشة لإدارة وظائف محددة للجسر: الوصول إلى أداة المساعدة المستندة إلى ويب والنسخ الاحتياطي لملف التكوين وإعادة التمهيد.



Management (إدارة)

Bridge Access (الوصول إلى الجسر)

استخدم كلمة مرور لحماية الوصول إلى أداة المساعدة المستندة إلى مستعرض.

Bridge Password (كلمة مرور الجسر) أدخل كلمة مرور جديدة للجسر.

Re-enter to confirm (إعادة الإدخال للتأكيد) أدخِل كلمة المرور مجدداً للتأكيد.

Idle Timeout (مهلة الخمول) تنتهي مهلة تسجيل الدخول بعد مدة الخمول التي تحددها. يتراوح النطاق ما بين **60** و **3600** ثانية. الإعداد الافتراضي هو **600**.

Web Access (الوصول إلى ويب)

Access via Wireless (الوصول لاسلكياً) إذا كنت تستخدم الجسر في نطاق عام حيث تقوم بتوفير الوصول اللاسلكي لضيوفك، فيمكنك تعطيل الوصول اللاسلكي إلى أداة المساعدة المستندة إلى مستعرض الخاصة بالجسر. ستكون قادراً فقط على الوصول إلى أداة المساعدة المستندة إلى مستعرض عبر اتصال سلكي إذا قمت بتعطيل هذا الإعداد. أبقِ على الإعداد الافتراضي، **Enabled (ممكّن)**، للسماح بالوصول اللاسلكي إلى أداة المساعدة المستندة إلى مستعرض الخاصة بالجسر، أو حدد **Disabled (معطّل)** لحظر الوصول اللاسلكي إلى أداة المساعدة.

Backup and Restore (النسخ الاحتياطي والاستعادة)

Backup (النسخ الاحتياطي) لنسخ ملف تكوين الجسر احتياطياً، انقر فوق **Backup Configurations (نسخ التكوينات احتياطيا)**. ثمّ اتبع الإرشادات التي تظهر على الشاشة.

Restore (الاستعادة) انقر فوق **Browse (استعراض)** وحدد ملف التكوين. ثم انقر فوق **Restore Configurations (استعادة التكوينات)**.

System Reboot (إعادة تمهيد النظام)

Reboot (إعادة التمهيد) لإعادة تمهيد الجسر أو إعادة تشغيله. انقر فوق **Start to Reboot (بدء إعادة التمهيد)**.

انقر فوق **Save Settings (حفظ الإعدادات)** لتطبيق التغييرات أو انقر فوق **Cancel Changes (إلغاء التغييرات)** لإلغاء التغييرات.

Administration (الإدارة) > Factory Defaults (الإعدادات الافتراضية للشركة المصنّعة)

استخدم هذه الشاشة لاستعادة تكوين الجسر إلى الإعدادات الافتراضية للشركة المصنّعة.

Factory Defaults (الإعدادات الافتراضية للشركة المصنّعة)

Restore All Settings (استعادة كل الإعدادات) لإعادة تعيين إعدادات الجسر إلى الإعدادات الافتراضية للشركة المصنّعة. انقر فوق **Restore All Settings (استعادة كل الإعدادات)**. ستخسر أي إعدادات سبق أن قمت بحفظها عند استعادة الإعدادات الافتراضية.



Administration (الإدارة) > Upgrade Firmware (ترقية البرنامج الثابت)

استخدم هذه الشاشة لترقية البرنامج الثابت الخاص بالجسر. لا تقم بترقية البرنامج الثابت إلا إذا كنت تواجه مشاكل مع الجسر أو إذا كان البرنامج الثابت الجديد يتضمن ميزة تريد استخدامها.



قبل ترقية البرنامج الثابت، قم بتنزيل ملف ترقية البرنامج الثابت الخاص بالجسر من موقع ويب الخاص بـ Linksys www.Linksys.com/support.

Upgrade Firmware (ترقية البرنامج الثابت)

Please select a file to upgrade the firmware (يرجى تحديد ملف لترقية البرنامج الثابت) انقر فوق **Browse (استعراض)** وحدد ملف ترقية البرنامج الثابت. ثم انقر فوق **Start to Upgrade (بدء الترقية)** واتبع التعليمات التي تظهر على الشاشة.

Status (الحالة) > Bridge (الجسر)

يتم عرض معلومات الحالة الحالية للجسر.



Bridge Information (معلومات الجسر)

Firmware Version (إصدار البرنامج الثابت) يتم عرض البرنامج الثابت الحالي للجسر.

Local Network (الشبكة المحلية)

Local MAC Address (عنوان MAC المحلي) يتم عرض عنوان MAC الخاص بالجسر كما يظهر على شبكة Ethernet المحلية.

IP Address (عنوان IP) يتم عرض عنوان IP الخاص بالجسر كما يظهر على شبكة Ethernet المحلية.

Subnet Mask (قناع الشبكة الفرعية) يتم عرض قناع الشبكة الفرعية الذي تم تكوينه لشبكتك المحلية.

Status (الحالة) > Wireless (اللاسلكي)

يتم عرض معلومات حول شبكتك اللاسلكية.



Wireless (اللاسلكي)

Link Status (حالة الارتباط) يتم عرض حالة الاتصال بشبكتك اللاسلكية.

MAC Address (عنوان MAC) يتم عرض عنوان MAC الخاص بالجسر كما يظهر على شبكتك اللاسلكية المحلية.

Network Name (SSID) (اسم الشبكة (SSID)) يتم عرض اسم الشبكة اللاسلكية أو SSID.

BSSID يتم عرض عنوان MAC اللاسلكي للموجّه اللاسلكي المتصل (أو نقطة الوصول).

Radio Band (نطاق التردد اللاسلكي) يتم عرض نطاق التردد اللاسلكي لشبكتك اللاسلكية.

Channel Width (عرض القناة) يتم عرض عرض القناة، بالميغا هرتز، الذي تستخدمه شبكتك اللاسلكية.

Wide Channel (القناة الواسعة) تبعاً لإعدادات القناة الخاصة بموجّه الشبكة، يتم عرض القناة الواسعة. إذا قمت بتحديد Wide - 40MHz Channel (قناة 40 ميغا هرتز - واسعة) لإعداد Radio Band (نطاق التردد اللاسلكي) أو Channel Width (عرض القناة) للموجّه، فستكون هذه هي قناة لاسلكي-N الأساسية الخاصة بك.

Standard Channel (القناة القياسية) يتم عرض إعداد القناة القياسية. إذا قمت بتحديد Wide - 40MHz Channel (قناة 40 ميغا هرتز - واسعة) لإعداد Radio Band (نطاق التردد اللاسلكي) أو Channel Width (عرض القناة) للموجّه، فستكون القناة القياسية هي قناة ثانوية للاسلكي-N.

Bit Rate (سرعة البت) يتم عرض سرعة إرسال البيانات.

Signal (الإشارة) يتم عرض النسبة المئوية لقوة الإشارة. 100% هي أعلى قوة إشارة ممكنة، و0% هي أضعف إشارة ممكنة.

Security (الأمان) يتم عرض أسلوب الأمان الخاص بشبكتك اللاسلكية.

استكشاف الأخطاء وإصلاحها

WES610N/WET610N

يتعذر على الكمبيوتر أو جهاز Ethernet سلكي آخر الاتصال بالموجّه اللاسلكي.

1. قم بالوصول إلى أداة المساعدة المستندة إلى مستعرض الخاصة بالجسر.
2. في شاشة *Basic Wireless Settings (الإعدادات اللاسلكية الأساسية)*، تأكد من أن Network Name (SSID) (اسم الشبكة (SSID)) مطابق لاسم شبكتك اللاسلكية.
3. تأكد من أن إعدادات الأمان (WPA أو WPA2 أو WEP) مطابقة لإعدادات الأمان الخاصة بشبكتك اللاسلكية.

عنوان IP الخاص بالجسر بحاجة إلى تغيير.

إذا كان الجسر متصلاً بشبكة مزوّدة بخادم DHCP (عادة موجّه الشبكة)، فسيحصل الجسر على عنوان IP من خادم DHCP. في حالة عدم وجود خادم DHCP، سيستخدم الجسر عنوان IP الثابت الافتراضي الخاص به، **169.254.1.250**.

إذا كنت تريد أن يستخدم الجسر عنوان IP ثابتاً دائماً، فاتبع هذه التعليمات:

1. قم بالوصول إلى أداة المساعدة المستندة إلى مستعرض الخاصة بالجسر.
2. انقر فوق علامة التبويب **Network Setup (إعداد الشبكة)**.
3. من القائمة المنسدلة *Network Connection Type (نوع اتصال الشبكة)*، حدد **Static IP (IP ثابت)**.
4. أكمل الحقول *Static IP Address (عنوان IP ثابت)* و*Subnet Mask (قناع الشبكة الفرعية)* و*Default Gateway (العبّارة الافتراضية)*.
5. انقر فوق **Save Settings (حفظ الإعدادات)**.

لن يتصل الكمبيوتر الممكّن به الجسر أو جهاز Ethernet سلكي آخر بجهاز آخر ممكّنة به خاصية الاتصال اللاسلكي (مثل كمبيوتر أو طابعة).

يرجى التحقق ممّا يلي:

- تأكد من أن الجهاز الممكّنة به خاصية الاتصال اللاسلكي موجود على الشبكة اللاسلكية نفسها الموجود عليها الكمبيوتر أو جهاز Ethernet السلكي الآخر المتصل بالجسر.
- تأكد من استخدام اسم الشبكة (SSID) نفسه لكافة الأجهزة الموجودة على الشبكة اللاسلكية.
- تأكد من وجود كافة الأجهزة على شبكة IP نفسها، باستخدام عناوين IP متوافقة.

لا تقبل أداة المساعدة المستندة إلى مستعرض كلمة المرور.

يرجى التحقق ممّا يلي:

- كلمة المرور متحسّسة لحالة الأحرف. تأكّد من استخدام الحرف (الأحرف) الصحيح (الصحيحة) عند إدخال كلمة المرور.
- إذا نسيت كلمة المرور، فيمكن إعادة تعيين الجسر إلى الإعدادات الافتراضية للشركة المصنّعة.

 اضغط باستمرار على زر **إعادة التعيين** الخاص بالجسر لمدة خمس ثوانٍ تقريباً. وستتم إعادة تعيين كلمة المرور إلى الإعداد الافتراضي للشركة المصنّعة، **admin**. ستتم أيضاً إعادة تعيين كافة إعدادات الجسر الأخرى إلى الإعدادات الافتراضية للشركة المصنّعة. (للوصول إلى أداة المساعدة المستندة إلى مستعرض، أدخل **admin** في حقل *Password (كلمة المرور)*.)

بعد قيامك بالتغييرات اللازمة من خلال أداة المساعدة المستندة إلى مستعرض، لن يتم عرض الإعدادات الجديدة على الشاشة.

في مستعرض ويب انقر فوق **Refresh (تحديث)**. في حال لم يتم عرض الإعدادات الجديدة، اتبع هذه التعليمات:

1. افصل محوّل الطاقة من الجسر.
2. انتظر خمس ثوانٍ، ثم أعد توصيل محوّل الطاقة بالجسر.
3. في مستعرض ويب انقر فوق **Refresh (تحديث)**.

ويب

إذا لم تتم معالجة أسئلتك هنا، فيُرجى الرجوع إلى موقع Linksys على ويب **Linksys.com/support**

المواصفات

WES610N

الطراز	WES610N
المعايير	IEEE 802.3u، 802.11g، 802.11b، 802.11a، 802.11n
الأضواء	الطاقة وEthernet وWi-Fi Protected Setup™، اللاسلكي، ونشاط وارتباط Ethernet الفردي
المنافذ	Ethernet (4)، الطاقة
الأزرار	إعادة التعيين، الإعداد المحمي بتقنية Wi-Fi
نوع الكبلات	CAT5e
أجهزة الهوائي	3 (داخلية)
نوع موصل الهوائي	غير متوفر
قابل للفصل (نعم/لا)	لا
التعديلات	802.11a: OFDM/BPSK، QPSK، 16-QAM، 64-QAM 802.11b: CCK/QPSK، BPSK 802.11g: OFDM/BPSK، QPSK، 16-QAM، 64-QAM 802.11n: OFDM/BPSK، QPSK، 16-QAM، 64-QAM
طاقة التردد اللاسلكي (EIRP) بالديسيبل/ميللي واط	802.11a: 15 ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11b: 19 ديسيبل/ميللي واط (نموذجي) @ 11 ميغابت بالثانية 802.11g: 16 ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11n (2.4 غيغا هرتز): 18 ديسيبل/ميللي واط (نموذجي) @ MCS15 802.11n (5 غيغا هرتز): 16 ديسيبل/ميللي واط (نموذجي) @ MCS15
حساسية التلقي	802.11a: 72- ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11b: 85- ديسيبل/ميللي واط (نموذجي) @ 11 ميغابت بالثانية 802.11g: 73- ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11n (20 ميغا هرتز): 75- ديسيبل/ميللي واط (نموذجي) @ MCS15 802.11n (40 ميغا هرتز): 69- ديسيبل/ميللي واط (نموذجي) @ MCS15
امتداد الهوائي بالديسيبل نسبة إلى هوائي آيزوتروبي	1
الأمان اللاسلكي	WEP، Wi-Fi Protected Access™ (WPA)، Wi-Fi Protected Access™ 2 (WPA2)
بتات مفتاح الأمان	تشفير يصل إلى 128 بت

المعطيات البيئية

المقاييس	6.97 × 5.04 × 2.68 بوصة (177 × 128 × 68 مم)
الوزن	0.65 رطل (295 غرام)
الشهادات	FCC، UL/cUL، ICES-003، RSS210، CE، Wi-Fi (IEEE 802 11a/b/g/draft n)، WPA2™، الإعداد المحمي بتقنية Wi-Fi، WMM®
الطاقة	12 فولت، 1 أمبير
درجة حرارة التشغيل	32 إلى 104 درجات فهرنهايت (0 إلى 40 درجة مئوية)
درجة حرارة التخزين	4- إلى 140 درجة فهرنهايت (20- إلى 60 درجة مئوية)
نسبة الرطوبة أثناء التشغيل	من 10 إلى 85% من دون تكاثف
نسبة الرطوبة أثناء التخزين	من 5 إلى 90% من دون تكاثف

يمكن أن تخضع المواصفات للتغيير من دون إشعار.

WET610N

الطراز	WET610N
المعايير	IEEE 802.3u، 802.11g، 802.11b، 802.11a، 802.11n
الأضواء	الطاقة، Ethernet، Wi-Fi Protected Setup™، اللاسلكي
المنافذ	Ethernet والطاقة
الأزرار	إعادة التعيين، الإعداد المحمي بتقنية Wi-Fi
نوع الكبلات	CAT5e
أجهزة الهوائي	3 (داخلية)
نوع موصل الهوائي	غير متوفر
قابل للفصل (نعم/لا)	لا
التعديلات	802.11a: OFDM/BPSK، QPSK، 16-QAM، 64-QAM 802.11b: CCK/QPSK، BPSK 802.11g: OFDM/BPSK، QPSK، 16-QAM، 64-QAM 802.11n: OFDM/BPSK، QPSK، 16-QAM، 64-QAM
طاقة التردد اللاسلكي (EIRP) بالديسيبل/ميللي واط	802.11a: 15 ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11b: 18 ديسيبل/ميللي واط (نموذجي) @ 11 ميغابت بالثانية 802.11g: 16 ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11n: 12 ديسيبل/ميللي واط (نموذجي) @ 130 ميغابت بالثانية (HT20)، 270 ميغابت بالثانية (HT40)
حساسية التلقي	802.11a: -72 ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11b: -85 ديسيبل/ميللي واط (نموذجي) @ 11 ميغابت بالثانية 802.11g: -73 ديسيبل/ميللي واط (نموذجي) @ 54 ميغابت بالثانية 802.11n: -70 ديسيبل/ميللي واط (نموذجي) @ MCS15/2.4 غيغا هرتز -69 ديسيبل/ميللي واط (نموذجي) @ MCS15/5.0 غيغا هرتز
امتداد الهوائي بالديسيبل نسبة إلى هوائي آيزوتروبي	1
الأمان اللاسلكي	WEP، Wi-Fi Protected Access™ (WPA)، Wi-Fi Protected Access™ 2 (WPA2)
بتات مفتاح الأمان	تشفير يصل إلى 128 بت

المعطيات البيئية

المقاييس	5.71 × 4.17 × 2.05 بوصة (145 × 106 × 52 م)
الوزن	5.61 أونصة (159 غرام)
الشهادات	FCC، UL/cUL، ICES-003، RSS210، CE، Wi-Fi (IEEE 802 11a/b/g/draft n)، WPA2™، الإعداد المحمي بتقنية Wi-Fi، WMM®
الطاقة	12 فولت، 1 أمبير
درجة حرارة التشغيل	32 إلى 104 درجات فهرنهايت (0 إلى 40 درجة مئوية)
درجة حرارة التخزين	-4 إلى 140 درجة فهرنهايت (-20 إلى 60 درجة مئوية)
نسبة الرطوبة أثناء التشغيل	من 10 إلى 85% من دون تكاثف
نسبة الرطوبة أثناء التخزين	من 5 إلى 90% من دون تكاثف

يمكن أن تخضع المواصفات للتغيير من دون إشعار.

Linksys.com/support

Cisco وشعار Cisco وLinksys هي علامات تجارية أو علامات تجارية مسجلة لـ Cisco و/أو الشركات التابعة لها في الولايات المتحدة والدول الأخرى.
توجد قائمة بالعلامات التجارية الخاصة بشركة Cisco على الموقع www.cisco.com/go/trademarks. كافة العلامات التجارية الأخرى الواردة في هذا المستند هي ملكية خاصة لأصحابها المعنيين.

حقوق الطبع والنشر © للعام 2011 لشركة Cisco و/أو الشركات التابعة لها. جميع الحقوق محفوظة.

3425-01249



Ръководство за потребителя

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Съдържание:

Общ преглед на продукта

Светодиоден панел 2
Панел на портовете 3

Настройки за безжична защита

Смяна на името на безжичната мрежа (SSID) по подразбиране 4
Смяна на паролата по подразбиране 4
Разрешаване на филтриране по MAC адреси 4
Разрешаване на шифриране 4

Общи насоки за мрежова защита 4
Допълнителни съвети за защита. 5

Разширено конфигуриране

Отваряне на базираната на браузър помощна програма . . .6
Setup (Настройки) > Basic Setup (Основни настройки) 7
Language (Език) 7
Network Setup (Настройки на мрежата) 7

Wireless (Безжични) > Basic Wireless Settings (Основни безжични настройки) 7
Basic Wireless Settings (Основни безжични настройки) 8
Защита на безжичната мрежа 8
Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка) 9

Безжична мрежа > Обзор на сайта за безжични мрежи . . .10
Обзор на сайта за безжични мрежи 10

Безжична мрежа > WMM® 11
WMM 12

Wireless (Безжична мрежа) > Advanced Wireless Settings (Разширени безжични настройки) 13
Разширени безжични настройки 14

Administration (Администриране) > Management (Управление). 14
Management (Управление) 15

Administration (Администриране) > Factory Defaults (Фабрични настройки) 15
Factory Defaults (Фабрични настройки) 15

Administration (Администриране) > Upgrade Firmware (Надстройка на фърмуер) 15
Upgrade Firmware (Надстройка на фърмуер) 16

Status (Състояние) > Bridge (Мост). 16
Bridge Information (Информация за моста) 16
Local Network (Локална мрежа) 16

Status (Състояние) > Wireless (Безжична мрежа) 16
Wireless (Безжична мрежа) 16

Отстраняване на неизправности

WES610N/WET610N 17

Спецификации

WES610N 18
WET610N 19

Общ преглед на продукта

Благодарим ви, че избрахте Linksys Dual-Band N Entertainment Bridge. Чрез моста всяко кабелно Ethernet устройство може да се свърже с вашата безжична мрежа. Мостът е базиран на Wireless-N с двоен обхват, следователно е съвместим с всеки Wireless-N, -G, -A или -B рутер или точка за достъп. При инсталиране за първи път следвайте стъпките на обложката на компактдиска. За удобство при конфигурация на разширени настройки използвайте базираната на браузър помощна програма.

Светодиоден панел



WES610N WET610N

Wireless (Безжична мрежа) (синьо) Светодиодът за безжична мрежа свети, когато има безжична връзка. Светодиодът примигва, когато мостът активно изпраща или получава данни по безжичната мрежа.

Wi-Fi Protected Setup Button (Бутон за защитено конфигуриране на безжична връзка) Ако вашият рутер поддържа Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка) и използва защита WPA или WPA2, можете да използвате Wi-Fi Protected Setup за автоматично свързване на моста. За да използвате Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка), вж. "Wireless (Безжични) > Basic Wireless Settings (Основни безжични настройки)" на страница 7.

Wi-Fi Protected Setup LED (Светодиод за защитено конфигуриране на безжична връзка) (синьо/кехлибарено) Светодиодът примигва в синьо в продължение на две минути по време на конфигурирането на безжична връзка. Той светва в синьо при ак`ивиране на защитата на безжичната мрежа. Ако е настъпила грешка по време на процеса на Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка), светодиодът светва в кехлибарено. Проверете дали мрежовият рутер поддържа Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка). Изчакайте, докато светодиодът угасне, и след това опитайте отново.

Ethernet (синьо) Светодиодът за Ethernet свети, когато има кабелна връзка. Светодиодът примигва, когато мостът активно изпраща или получава данни чрез Ethernet порта (портовете).

Power (Захранване) (синьо) Светодиодът за захранване светва при включване на захранването на моста.

Панел на портовете



WES610N WET610N

Ethernet Ethernet портът (портовете) свързва моста с компютър или друго Ethernet мрежово устройство. WES610N е с четири порта, а WET610N - с един-единствен порт.

Reset (Нулиране) Съществуват два начина за нулиране на моста до фабричните му настройки. Можете да натиснете и задържите бутона за нулиране за прибл. пет секунди или да възстановите фабричните настройки от Administration (Администриране) > Factory Defaults (Фабрични настройки) в базираната на браузър помощна програма. Бутонът за нулиране на WES610N се намира на дъното му, а този на WET610N - на задния панел с портове.

Power (Захранване) Портът за захранване свързва моста с включения адаптер за захранване.

Настройки за безжична защита

Безжичните мрежи са удобни и лесни за инсталиране, поради което все повече домове с високоскоростен Интернет достъп се снабдяват с тях. Тъй като при безжичното мрежово свързване осъществява връзка чрез изпращане на информация чрез радио вълни, то е по-уязвимо за външна намеса в сравнение с традиционните кабелни мрежи. Подобно на сигналите от клетъчните или безжичните телефони, сигналите от безжични мрежи могат също да бъдат прихванати. Тъй като физически е невъзможно да предотвратите свързване на външни лица към вашата безжична мрежа, трябва да вземете допълнителни мерки за осигуряване на нейната защита.

Смяна на името на безжичната мрежа (SSID) по подразбиране

Безжичните устройства са с фабрично зададено име на безжичната мрежа по подразбиране или Service Set Identifier (SSID). Това е името на вашата безжична мрежа, чиято дължина може да бъде до 32 знака. Безжичните устройства на Linksys използват **linksys** като име на безжичната мрежа по подразбиране. Би трябвало да смените името на безжичната мрежа с уникално такова, което да позволява тя да се различава от другите съществуващи в близост безжични мрежи, но не използвайте лична информация (като напр. идентификационен номер), тъй като тази информация може да бъде достъпна за всеки, който осъществява търсене за безжични мрежи.

Смяна на паролата по подразбиране

За безжични устройства като точки за достъп и рутери от вас ще се иска парола, ако желаете да промените техните настройки. Тези устройства са с фабрично зададена парола по подразбиране. Паролата по подразбиране на Linksys е **admin**. Тези настройки по подразбиране са известни на хакерите и те могат да се опитат да ги използват, за да осъществят достъп до вашето безжично устройство и да променят мрежовите ви настройки. За да предотвратите неразрешени промени, персонализирайте паролата на устройството така, че да бъде трудно тя да бъде отгатната.

Разрешаване на филтриране по MAC адреси

Рутерите на Linksys ви дават възможност да разрешите филтриране по Media Access Control (MAC) адреси. MAC адресът представлява уникална поредица от цифри и букви, която се присвоява на всяко мрежово устройство. При разрешено филтриране по MAC адреси безжичен достъп се предоставя само на безжични устройства с конкретни MAC адреси. Например, ако укажете MAC адресите на всички компютри във вашия дом, само тези компютри ще имат достъп до вашата безжична мрежа.

Разрешаване на шифриране

Чрез шифрирането се осигурява защита на данните, предавани по безжична мрежа. Wi-Fi Protected Access (WPA/WPA2) и Wired Equivalent Privacy (WEP) осигуряват различни нива на защита при безжичното свързване.

Мрежа с WPA/WPA2 шифриране е по-защитена от такава с WEP шифриране, тъй като WPA/WPA2 използва шифриране с динамичен ключ. За да защитите информацията, която се предава в ефира, трябва да разрешите най-високото ниво на шифриране, поддържано от вашите мрежови устройства.

WEP е по-стар стандарт за шифриране и може да бъде единствената налична опция при някои по-стари устройства, които не поддържат WPA.

Общи насоки за мрежова защита

Безжичната мрежова защита е безполезна, ако стоящата в основата ѝ мрежа не е защитена.

- Защитата на всички компютри в мрежата се осъществява чрез парола, а файловете с чувствителна информация се защитават с индивидуални пароли.
- Сменяйте редовно паролите.
- Инсталирайте антивирусен софтуер и лична защитна стена.
- Забранете споделянето на файлове (при равноправен достъп). Някои приложения могат да отварят споделяне на файлове без ваше съгласие и/или знание.

Допълнителни съвети за защита

- Дръжте безжичните рутери, точки за достъп или шлюзове далеч от външни стени и прозорци.
- Изключвайте безжичните рутери, точки за достъп или шлюзове, когато не се използват (през нощта, по време на ваканция).
- Използвайте сигурни пароли с дължина от поне осем знака. Съчетавайте букви и цифри, за да избегнете употребата на стандартни думи, които могат да бъдат намерени в речниците.

Разширено конфигуриране

След инсталирането на моста, като следвате стъпките в обложката на компактдиска, мостът ще бъде готов за използване. Ако обаче искате да промените разширените му настройки, използвайте базираната на браузър помощна програма на моста. В тази глава се описва всяка уеб страница на помощната програма и ключовите функции на всяка страница. Можете да отворите помощната програма чрез уеб браузър на компютър, свързан с моста в мрежа.

Базираната на браузър помощна програма има следните основни раздели: Setup (Настройки), Wireless (Безжична мрежа), Administration (Администриране) и Status (Състояние). След като щракнете върху един от основните раздели, ще се появят допълнителни раздели.

Отваряне на базираната на браузър помощна програма

С помощта на браузър отворете базираната на браузър помощна програма.

Ако мостът е свързан към мрежа с DHCP сървър (обикновено мрежов рутер), то мостът ще получи своя IP адрес от DHCP сървъра. Ако няма DHCP сървър, мостът ще използва своя статичен IP адрес по подразбиране - **169.254.1.250**. (Ако зададете перманентен статичен IP адрес на моста посредством базираната на браузър помощна програма, вместо това въведете статичния IP адрес.)

ЗАБЕЛЕЖКА
Ако не знаете IP адреса на моста, намерете го в таблицата на DHCP клиентите на вашия рутер. (Вижте в документацията за рутера.)

Ако не можете да намерите IP адреса на моста, можете да нулирате моста; натиснете бутона **Reset** (Нулиране) на моста за около пет секунди, като използвате изправен кламер. С това мостът ще се върне обратно на фабричните си настройки. Мостът ще поиска IP адрес от DHCP сървъра (обикновено мрежовия рутер). Ако не се намери DHCP сървър, мостът ще използва статичния IP по подразбиране **169.254.1.250**, докато не открие DHCP сървър и не получи динамичен IP адрес.

Ако мостът не е свързан с рутер и използва фабричните настройки, свържете компютър към моста, като използвате Ethernet връзка за достъп до уеб-базираната помощна програма. Ще трябва да да конфигурирате Ethernet връзката на компютъра със статичен IP адрес и подмрежова маска.

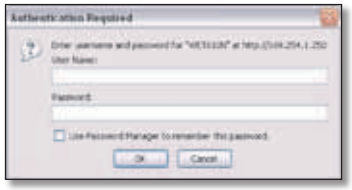
IP адресът на вашия Ethernet адаптер трябва да се зададе на конкретен IP адрес.

1. В полето *IP address* (IP адрес) въведете **169.254.x.y** (x трябва да се замести с число от 1 до 254, а y трябва да се замести с число от 0 до 255).
2. В полето *Subnet mask* (Подмрежова маска) въведете **255.255.0.0**.

ЗАБЕЛЕЖКА
Стъпките за присвояване на IP адрес на Ethernet адаптера на вашия компютър зависят от операционната система. За инструкции проверете в помощната документация на съответната операционна система.

След като присвоите на вашия Ethernet адаптер статичен IP адрес, стартирайте уеб браузъра и въведете IP адреса на адаптера (настройката по подразбиране е **169.254.1.250**) в полето *Address* (Адрес). Натиснете **Enter**.

Появява се екран за искане на парола. (Подобен екран ще видят и потребителите, които не са с Windows XP.) Оставете полето *User name* (Потребителско име) празно. Въведете паролата, която сте създали при използването на съветника за инсталиране. Ако не сте създали нова парола, използвайте паролата по подразбиране **admin**. (Можете да зададете нова парола от екрана *Administration* (Администриране) > *Management* (Управление). Натиснете **OK**, за да продължите.



ЗАБЕЛЕЖКА
Ако екранът за искане на парола не се появи, изчакайте две минути и опитайте отново.

Setup (Настройки) > Basic Setup (Основни настройки)

Първият екран, който се появява, е *Basic Setup* (Основни настройки). Използвайте този екран, за да смените езика на базираната на браузър помощна програма или да промените настройките на кабелната Ethernet мрежа на моста.





Language (Език)

Language (Език) Използва се, за да се зададе езикът, показван в базираната на браузър помощна програма. Изберете желания език от падащото меню.

Network Setup (Настройки на мрежата)

В този раздел се определя дали IP адресът се получава автоматично от DHCP сървър, например вашия мрежов рутер (Автоматично конфигуриране - DHCP), или се задава ръчно (Статичен IP).

Bridge IP (IP на мост) Ако мрежата има DHCP сървър, например вашия мрежов рутер, присвояващ IP адреси на мрежовите устройства, запазете настройката по подразбиране, **Automatic Configuration - DHCP** (Автоматично конфигуриране - DHCP). Мостът ще поиска IP адрес от DHCP сървъра (обикновено мрежовия рутер). Ако не се намери DHCP сървър, мостът ще използва статичния IP по подразбиране **169.254.1.250**, докато открие DHCP сървър и получи динамичен IP адрес.

Ако искате да зададете перманентен статичен адрес на моста, изберете **Static IP** (Статичен IP).

Ако изберете Static IP (Статичен IP), попълнете следните полета:

- **Static IP Address** (Статичен IP адрес) Въведете уникален IP адрес, който ще бъде използван за достъп до базираната на браузър помощна програма.
- **Subnet Mask** (Подмрежова маска) Въведете подмрежовата маска на вашата кабелна мрежа.
- **Default Gateway** (Шлюз по подразбиране) Въведете IP адреса на шлюза по подразбиране за вашата мрежа (в повечето случаи това е вашият рутер).

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Wireless (Безжични) > Basic Wireless Settings (Основни безжични настройки)

Използвайте екрана *Basic Wireless Settings* (Основни безжични настройки), за да конфигурирате основните безжични и защитни настройки на моста.

Има два начина за конфигуриране на настройките на моста - ръчно и чрез Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка). Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка) е функция, която улеснява настройването на безжичната мрежа. Ако вашият рутер поддържа Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка) и използва защита WPA или WPA2, можете да използвате Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка) за автоматично свързване на моста.

Configuration View (Изглед на конфигуриране) За да конфигурирате ръчно своята безжична мрежа, изберете **Manual** (Ръчно). Вж. **Basic Wireless Settings** (Основни безжични настройки), **страница 8**. За да използвате Wi-Fi Protected Setup, изберете **Wi-Fi Protected Setup** (Защитено конфигуриране на безжична връзка). Вж. **Wi-Fi Protected Setup** (Защитено конфигуриране на безжична връзка), **страница 9.**

Basic Wireless Settings (Основни безжични настройки)



Network Name (SSID) (Име на мрежата - SSID) SSID е името на мрежата, споделяно от всички точки в дадена безжична мрежа. SSID трябва да е едно и също за всички устройства в безжичната мрежа. То е чувствително към главни и малки букви и не трябва да надвишава 32 знака (използват се всички знаци на клавиатурата). Уверете се, че тази настройка е същата като настройката на вашия безжичен рутер или точка за достъп. За допълнителна защита трябва да смените даденото по подразбиране име SSID (**linksys**) с уникално име.

Защита на безжичната мрежа

Мостът поддържа следните опции на защита на безжичната мрежа: WPA лична, WPA2 лична и WEP. WPA (Wi-Fi Protected Access) и WPA2 са по-сигурни методи на защита от WEP (Wired Equivalent Privacy). За допълнителна информация за защитата на безжичната мрежа вижте "Настройки за безжична защита", страница 4.

Режим на защита

Изберете метода на защита за безжичната си мрежа. Ако не искате да използвате защита на безжичната мрежа, запазете стойността по подразбиране **Disabled** (Деактивиран).

ЗАБЕЛЕЖКА
Запомнете, че всички устройства във вашата безжична мрежа ТРЯБВА да използват един и същ метод и парола/ключ на защита, защото в противен случай безжичните устройства няма да могат да комуникират помежду си.

WPA лична

WPA е стандарт за защита, по-сигурен от шифроването на WEP.



Encryption (Шифроване) WPA поддържа метода на шифроване TKIP с динамични ключове на шифроване.

Passphrase (Парола) Въведете ключа, който е общ за моста и вашия безжичен рутер или точка за достъп. Той трябва да е съставен от 8-63 знака.

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

WPA2 лична

WPA2 е по-усъвършенствана и по-сигурна версия на WPA.



Encryption (Шифроване) WPA2 поддържа два метода на шифроване, TKIP и AES, с динамични ключове на шифроване. Изберете метод на шифроване, **AES** или **TKIP или AES**. Избраният по подразбиране метод е **AES**.

Passphrase (Парола) Въведете ключа, който е общ за моста и вашия безжичен рутер или точка за достъп. Той трябва да е съставен от 8-63 знака.

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

WEP

WEP е базисен метод на шифроване, който не е толкова сигурен, колкото WPA или WPA2.



Encryption (Шифроване) Изберете ниво на WEP шифроване, **40/64 bits (10 hex digits)** (40/64 бита (10 шестнайсетични числа)) или **104/128 bits (26 hex digits)** (104/128 бита (26 шестнайсетични числа)). По подразбиране това е **40/64 bits (10 hex digits)** (40/64 бита (10 шестнайсетични числа)).

Key 1 Въведете WEP ключа на вашата мрежа.

Tx Key **Key 1** (Ключ 1) е предавателният ключ, използван от моста.

Authentication (Удостоверяване) По подразбиране е **Auto** (Авто), което позволява да се използва удостоверяване чрез отворена система или чрез споделен ключ. Изберете **Open** (Отворена), за да използвате удостоверяване чрез отворена система; подателят и получателят не използват WEP ключ за удостоверяване. Изберете **Shared** (Споделен), за да използвате удостоверяване чрез споделен ключ; подателят и получателят използват WEP ключ за удостоверяване.

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка)

Съществуват два метода. Използвайте метода, който е приложим за вашия рутер.





Метод #1

Използвайте този метод, ако вашият рутер има бутон за защитено конфигуриране на безжична връзка.

1. Щракнете върху или натиснете бутона **Wi-Fi Protected Setup** (Защитено конфигуриране на безжична връзка) на рутера.
2. В рамките на две минути щракнете върху бутона **Wi-Fi Protected Setup** (Защитено конфигуриране на безжична връзка) на екрана *Wi-Fi Protected Setup* (Защитено конфигуриране на безжична връзка) на моста.
3. След конфигурирането на моста щракнете върху **Close** (Затваряне).

На екрана *Wi-Fi Protected Setup* се показват състоянието на връзката, името на мрежата (SSID) и методът на защита.

Метод #2

Използвайте този метод, ако вашият рутер изисква PIN кода на моста.

1. На **екрана** *Wi-Fi Protected Setup* (Защитено конфигуриране на безжична връзка) на рутера въведете PIN кода на **екрана** *Wi-Fi Protected Setup* (Защитено конфигуриране на безжична връзка) на моста. След това щракнете върху **Register** (Регистриране) или на съответния бутон. (Той е посочен също така на етикета на дъното на моста.)
2. На **екрана** *Wi-Fi Protected Setup* (Защитено конфигуриране на безжична връзка) на моста щракнете върху **OK**.
3. След конфигурирането на моста щракнете върху **Close** (Затваряне).

На екрана *Wi-Fi Protected Setup* (Защитено конфигуриране на безжична връзка) се показват състоянието на връзката, името на мрежата (SSID) и методът на защита.

Безжична мрежа > Обзор на сайта за безжични мрежи

Щракнете върху раздела **Wireless Network Site Survey** (Обзор на сайта за безжични мрежи), за да започнете обзор на сайта. На екрана *Wireless Network Site Survey* (Обзор на сайта за безжични мрежи) се показват откритите от моста безжични мрежи.



Обзор на сайта за безжични мрежи

Number of Wireless Networks (Брой безжични мрежи) Показва се броят на откритите от моста безжични връзки.

Select (Избор) За свързване с безжична мрежа щракнете върху **Select** (Избор). След това щракнете върху **Connect** (Свързване).

Wireless Network Name (Име на безжична мрежа) Показва се името на безжичната мрежа (SSID).

GHz Показва се радио обхватът на безжичната мрежа.

Signal (Сигнал) Показва се силата на сигнала (в проценти). 100% е най-голямата възможна сила на сигнала; 0% е най-малката възможна сила на сигнала.

Security (Защита) Ако мрежата поддържа Wi-Fi Protected Setup (Защитено конфигуриране на безжична връзка), се показва иконата на защитено конфигуриране на безжична връзка . Показва се методът на защита, който се използва от безжичната мрежа.

Щракнете върху **Refresh** (Обновяване), за да актуализирате информацията на екрана.

След избора на мрежа щракнете върху **Connect** (Свързване). Появява се нов екран. Следвайте инструкциите за метода на защита на вашата мрежа.

WPA



Network Name (SSID) (Име на мрежата - SSID) Автоматично се показва името на избраната от вас мрежа.

Security Mode (Режим на защита) Автоматично се показва WPA Personal (WPA лична).

Encryption (Шифроване) WPA поддържа метода на шифроване TKIP с динамични ключове на шифроване.

Passphrase (Парола) Въведете ключа, който е общ за моста и вашия безжичен рутер или точка за достъп. Той трябва да е съставен от 8-63 знака.

Щракнете върху **Refresh** (Обновяване), за да актуализирате информацията на екрана.

След въвеждане на настройките за защита щракнете върху **Connect** (Свързване).

WPA2



Network Name (SSID) (Име на мрежата - SSID) Автоматично се показва името на избраната от вас мрежа.

Security Mode (Режим на защита) Автоматично се показва WPA Personal (WPA-личен).

Encryption (Шифроване) WPA2 поддържа два метода на шифроване, TKIP и AES, с динамични ключове на шифроване. Изберете метод на шифроване, **AES** или **TKIP or AES** (TKIP или AES).

Passphrase (Парола) Въведете ключа, който е общ за моста и вашия безжичен рутер или точка за достъп. Той трябва да е съставен от 8-63 знака.

Щракнете върху **Refresh** (Обновяване), за да актуализирате информацията на екрана.

След въвеждане на настройките за защита щракнете върху **Connect** (Свързване).

WEP



Network Name (SSID) (Име на мрежата - SSID) Автоматично се показва името на избраната от вас мрежа.

Security Mode (Режим на защита) Автоматично се показва WEP.

Encryption (Шифроване) Изберете ниво на WEP шифроване, **40/64 bits (10 hex digits)** (40/64 бита (10 шестнайсетични числа)) или **104/128 bits (26 hex digits)** (104/128 бита (26 шестнайсетични числа)).

Key 1 Въведете WEP ключа на вашата мрежа.

Tx Key **Key 1** (Ключ 1) е предавателният ключ, използван от моста.

Authentication (Удостоверяване) По подразбиране е **Auto** (Авто), което позволява да се използва удостоверяване чрез отворена система или чрез споделен ключ. Изберете **Open** (Отворена), за да използвате удостоверяване чрез отворена система; подателят и получателят не използват WEP ключ за удостоверяване. Изберете **Shared** (Споделен), за да използвате удостоверяване чрез споделен ключ; подателят и получателят използват WEP ключ за удостоверяване.

Щракнете върху **Refresh** (Обновяване), за да актуализирате информацията на екрана.

След въвеждане на настройките за защита щракнете върху **Connect** (Свързване).

Безжична мрежа > WMM®

Конфигурирайте настройките на Wireless MultiMedia (WMM). WMM приоритизира пакетите в зависимост от съответния им режим на достъп (тип трафик): Background (Фонов), Best Effort (Най-добър възможен), Video (Видео) или Voice (Гласов). Тези настройки трябва да се регулират само от опитен администратор, тъй като неправилните настройки могат да се отразят неблагоприятно на безжичното свързване.



ЗАБЕЛЕЖКА
Настройките на *WMM* екрана са предназначени само за напреднали потребители.

WMM

Режим на достъп

Можете да присвоявате различни настройки на четирите налични режима на достъп. Изберете режима, който искате да конфигурирате. **Background** (Фонов), **Best Effort** (Най-добър възможен), **Video** (Видео) или **Voice** (Гласов). Следвайте инструкциите за избрания от вас режим.

Background (Фонов)

Use Aggregation (Използвай обединяване) Тази опция определя дали слоят за управление на достъпа до носители Media Access Control (MAC) ще настрои сесия за потвърждение на добавяне на блок Add Block Acknowledgement (ADDBA). По подразбиране това е **No** (Не). Изберете **Yes** (Да), за да разрешите тази опция.

Accept Aggregation (Приеми обединяване) Тази опция определя дали слоят за управление на достъпа до носители MAC ще приеме ADDBA заявка. По подразбиране това е **Yes** (Да). Изберете **No** (Не), за да забраните тази опция.

Max. Number of Packets in Aggregation (Макс. брой пакети в обединение) Тази опция определя максималния брой пакети (подрамки) в обединение. Обхватът е от **0** до **7**. Стойността по подразбиране е **7**.

Max. Aggregation Size (Макс. размер на обединение) Тази опция определя максималния размер на обединението (в байтове). Обхватът е от **0** до **16000**. Стойността по подразбиране е **12000**.

Timeout Internal (Вътрешно време на изчакване) Тази опция определя времето на изчакване, в рамките на което обединението трябва да бъде затворено със "затварящо условие", преди да бъде затворено от таймера. Обхватът е от **0** до **100**ms. Стойността по подразбиране е **3**.

Min. Size of Packet in Aggregation (Мин. размер на пакет в обединение) Тази опция определя минималния размер (в байтове) на пакетите, които ще се натрупват в обединението. Обхватът е от **0** до **1500**. Стойността по подразбиране е **10**.

ADDBA Timeout (Време на изчакване за ADDBA) Тази опция определя времето, след изтичането на което настройката ADDBA се прекратява, ако не настъпи обмен на кадри от споразумението за потвърждение на блок (ACK). Обхватът е от **0** до **65535** ms. Стойността по подразбиране е **0**, при която се отменя времето на изчакване.

Aggregation Window Size (Размер на прозорец за обединение) Тази опция определя максималния брой пакети, които могат да бъдат предавани без получаване на ACK. Обхватът е от **0** до **64**. Стойността по подразбиране е **64**.

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Best Effort (Най-добър възможен)

Use Aggregation (Използвай обединяване) Тази опция определя дали слоят за управление на достъпа до носители Media Access Control (MAC) ще настрои сесия за потвърждение на добавяне на блок (ADDBA). По подразбиране това е **Yes** (Да). Изберете **No** (Не), за да забраните тази опция.

Accept Aggregation (Приеми обединяване) Тази опция определя дали слоят за управление на достъпа до носители MAC ще приеме ADDBA заявка. По подразбиране това е **Yes** (Да). Изберете **No** (Не), за да забраните тази опция.

Max. Number of Packets in Aggregation (Макс. брой пакети в обединение) Тази опция определя максималния брой пакети (подрамки) в обединение. Обхватът е от **0** до **10**. Стойността по подразбиране е **10**.

Max. Aggregation Size (Макс. размер на обединение) Тази опция определя максималния размер на обединението (в байтове). Обхватът е от **0** до **20000**. Стойността по подразбиране е **16000**.

Timeout Internal (Вътрешно време на изчакване) Тази опция определя времето на изчакване, в рамките на което обединението трябва да бъде затворено със "затварящо условие", преди да бъде затворено от таймера. Обхватът е от **0** до **100**ms. Стойността по подразбиране е **3**.

Min. Size of Packet in Aggregation (Мин. размер на пакет в обединение) Тази опция определя минималния размер (в байтове) на пакетите, които ще се натрупват в обединението. Обхватът е от **0** до **1500**. Стойността по подразбиране е **10**.

ADDBA Timeout (Време на изчакване за ADDBA) Тази опция определя времето, след изтичането на което настройката ADDBA се прекратява, ако не настъпи обмен на кадри от споразумението за потвърждение на блок (ACK). Обхватът е от **0** до **65535** ms. Стойността по подразбиране е **0**, при която се отменя времето на изчакване.

Aggregation Window Size (Размер на прозорец за обединение) Тази опция определя максималния брой пакети, които могат да бъдат предавани без получаване на ACK. Обхватът е от **0** до **64**. Стойността по подразбиране е **64**.

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Видео

Use Aggregation (Използвай обединяване) Тази опция определя дали слоят за управление на достъпа до носители (MAC) ще настрои сесия за потвърждение на добавяне на блок Add Block Acknowledgement (ADDBA). По подразбиране това е **Yes** (Да). Изберете **No** (Не), за да забраните тази опция.

Accept Aggregation (Приеми обединяване) Тази опция определя дали слоят за управление на достъпа до носители MAC ще приеме ADDBA заявка. По подразбиране това е **Yes** (Да). Изберете **No** (Не), за да забраните тази опция.

Max. Number of Packets in Aggregation (Макс. брой пакети в обединение) Тази опция определя максималния брой пакети (подкадри) в обединение. Обхватът е от **0** до **7**. Стойността по подразбиране е **7**.

Max. Aggregation Size (Макс. размер на обединение) Тази опция определя максималния размер на обединението (в байтове). Обхватът е от **0** до **16000**. Стойността по подразбиране е **12000**.

Timeout Internal (Вътрешно време на изчакване) Тази опция определя времето на изчакване, в рамките на което обединението трябва да бъде затворено със "затварящо условие", преди да бъде затворено от таймера. Обхватът е от **0** до **100** ms. Стойността по подразбиране е **3**.

Min. Size of Packet in Aggregation (Мин. размер на пакет в обединение) Тази опция определя минималния размер (в байтове) на пакетите, които ще се натрупват в обединението. Обхватът е от **0** до **1500**. Стойността по подразбиране е **10**.

ADDBA Timeout (Време на изчакване за ADDBA) Тази опция определя времето, след изтичането на което настройката ADDBA се прекратява, ако не настъпи обмен на кадри от споразумението за потвърждение на блок (ACK). Обхватът е от **0** до **65535** ms. Стойността по подразбиране е **0**, при която се отменя времето на изчакване.

Aggregation Window Size (Размер на прозорец за обединение) Тази опция определя максималния брой пакети, които могат да бъдат предавани без получаване на ACK. Обхватът е от **0** до **64**. Стойността по подразбиране е **64**.

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Voice (Гласов)

Use Aggregation (Използвай обединяване) Тази опция определя дали слоят за управление на достъпа до носители Media Access Control (MAC) ще настрои сесия за потвърждение на добавяне на блок Add Block Acknowledgement (ADDBA). По подразбиране това е **Yes** (Да). Изберете **No** (Не), за да забраните тази опция.

Accept Aggregation (Приеми обединяване) Тази опция определя дали слоят за управление на достъпа до носители MAC ще приеме ADDBA заявка. По подразбиране това е **Yes** (Да). Изберете **No** (Не), за да забраните тази опция.

Max. Number of Packets in Aggregation (Макс. брой пакети в обединение) Тази опция определя максималния брой пакети (подкадри) в обединение. Обхватът е от **0** до **2**. Стойността по подразбиране е **2**.

Max. Aggregation Size (Макс. размер на обединение) Тази опция определя максималния размер на обединението (в байтове). Обхватът е от **0** до **16000**. Стойността по подразбиране е **10000**.

Timeout Internal (Вътрешно време на изчакване) Тази опция определя времето на изчакване, в рамките на което обединението трябва да бъде затворено със "затварящо условие", преди да бъде затворено от таймера. Обхватът е от **0** до **100** ms. Стойността по подразбиране е **10**.

Min. Size of Packet in Aggregation (Мин. размер на пакет в обединение) Тази опция определя минималния размер (в байтове) на пакетите, които ще се натрупват в обединението. Обхватът е от **0** до **1500**. Стойността по подразбиране е **10**.

ADDBA Timeout (Време на изчакване за ADDBA) Тази опция определя времето, след изтичането на което настройката ADDBA се прекратява, ако не настъпи обмен на кадри от споразумението за потвърждение на блок (ACK). Обхватът е от **0** до **65535** ms. Стойността по подразбиране е **0**, при която се отменя времето на изчакване.

Aggregation Window Size (Размер на прозорец за обединение) Тази опция определя максималния брой пакети, които могат да бъдат предавани без получаване на ACK. Обхватът е от **0** до **64**. Стойността по подразбиране е **64**.

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Wireless (Безжична мрежа) > Advanced Wireless Settings (Разширени безжични настройки)

Конфигурирайте разширените функции на моста за безжично свързване. Тези настройки трябва да се регулират само от опитен администратор, тъй като неправилните настройки могат да се отразят неблагоприятно на безжичното свързване.



ЗАБЕЛЕЖКА
Настройките на екрана *Advanced Wireless Settings* (Разширени безжични настройки) са предназначени само за напреднали потребители.

Разширени безжични настройки

Use LDPC (Използвай LDPC) Low-Density Parity-Check Code (LDPC) позволява или забранява корекцията на грешки с цел намаляване на вероятността от загуба на данни в шумни канали. Алгоритъмът за адаптиране на скоростта автоматично забранява LDPC кодиране, когато се работи с високи PHY скорости (по-високи от 162). За да използвате разширената LDCP схема за корекция на грешки, запазете настройката по подразбиране, **Yes** (Да). В противен случай изберете **No** (Не).

ERP Protection Type (Тип ERP защита) С тази опция се конфигурира защита на OFDM пакетите въпреки наличието на 802.11b станции в рамките на безжичната мрежа. Чрез изпращане на RTS/CTS или CTS2Self пакети с 802.11b скорости, мостът осведомява безжичната мрежа, че ще се прехвърлят OFDM пакети и осигурява защитата им в безжичната мрежа. RTS/CTS и CTS2Self пакетите създават служебни ресурси, което може да доведе до по-ниски скорости на предаване.

Опцията RTS/CTS осигурява по-добро покритие, но по-ниски скорости на предаване в сравнение с CTS2Self, тъй като опцията RTS/CTS включва потвърждение от приемащото устройство. За да използвате опцията RTS/CTS, запазете настройката по подразбиране, **RTS/CTS**. Опцията None (Няма) може да предизвика колизии между OFDM и CCK пакетите. За да използвате тази опция, изберете **None** (Няма). За да използвате опцията CTS2Self, изберете **CTS2Self**.

11n Protection Type (Тип 11n защита) С тази опция се конфигурира защита от устройства с ниски скорости на предаване (non-HT) в рамките на безжичната мрежа. В случай че безжичният рутер (точка за достъп) открие асоциация на наследено не-HT устройство, той ще изпрати сигнал на всички устройства с високи скорости на предаване (HT) да използват RTS/CTS или CTS2Self механизми преди всяко предаване на данни. Тази функция поддържа също така всички стандартни защити 802.11n, включително MIMO.

Опцията RTS/CTS осигурява по-добро покритие, но по-ниски скорости на предаване в сравнение с CTS2Self, тъй като опцията RTS/CTS включва потвърждение от приемащото устройство. За да използвате опцията RTS/CTS, запазете настройката по подразбиране, **RTS/CTS**. Опцията None (Няма) може да предизвика колизии между HT и наследените пакети. За да използвате тази опция, изберете **None** (Няма). За да използвате опцията CTS2Self, изберете **CTS2Self**.

Percentage of maximal transmit power (Максимална мощност на предаване - в проценти) С тази опция се задава максималната мощност на предаване (в проценти) по отношение на регулаторните ограничения на домейна. Например, ако регулаторните ограничения на домейна позволяват предаване до 20 dB, задаването на максималната мощност на предаване на 50% позволява максимално предаване на 10 dB. Изберете желаната от вас стойност в проценти. **12%**, **25%**, **50%** или **100%**. Стойността по подразбиране е **100%**.

QoS Classification Type (Тип QoS класификация) С тази опция се задава 802.1D или 802.1Q съпоставяне от полето IP DSCP/TOS до WMM приоритетите (Background, Best Effects, Video, Voice). Запазете стойността по подразбиране, **802.1D**, или изберете **802.1Q**, което се използва от някои IPTV потоци.

Re-establish Ethernet connection when initiating wireless connection (Повторно установяване на Ethernet връзка при инициализиране на безжична връзка) За да се задейства DHCP откриване от устройството, което стои зад моста, мостът ще нулира Ethernet връзката между моста и устройството при всяко установяване на безжична връзка. За да забраните това, изберете **No** (Не). В противен случай запазете стойността по подразбиране **Yes** (Да).

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Administration (Администриране) > Management (Управление)

Този екран се използва за управление на специфичните функции на моста: достъп до уеб базираната помощна програма, архивиране на конфигурационния файл и рестартиране.



Management (Управление)

Достъп до моста

Използвайте парола за защита на достъпа до базираната на браузър помощна програма.

Bridge Password (Парола на моста) Въведете нова парола за моста.

Re-enter to confirm (Повторно въвеждане за потвърждение) Въведете отново паролата, за да потвърдите.

Idle Timeout (Време на изчакване при неактивност) Автоматично излизане след указания от вас период на неактивност. Обхватът е от **60** до **3600** секунди. Стойността по подразбиране е **600**.

Web Access (Уеб достъп)

Access via Wireless (Достъп чрез безжична мрежа) Ако използвате моста в публичен домейн, в който предоставяте безжичен достъп на вашите гости, можете да забраните безжичния достъп до базираната на браузър помощна програма на моста. Ако забраните настройката, ще имате достъп до базираната на браузър помощна програма само чрез кабелна връзка. Запазете настройката по подразбиране **Enabled** (Активиран), за да разрешите безжичен достъп до базираната на браузър помощна програма на моста, или изберете **Disabled** (Деактивиран), за да забраните безжичния достъп до помощната програма.

Архивиране и възстановяване

Backup (Архивиране) За да архивирате конфигурационния файл на моста, щракнете върху **Backup Configurations** (Архивиране на конфигурациите). Следвайте инструкциите от екрана.

Restore (Възстановяване) Щракнете върху **Browse** (Преглед) и изберете конфигурационния файл. След това щракнете върху **Restore Configurations** (Възстановяване на конфигурациите).

Рестартиране на системата

Reboot (Рестартиране) За да презаредите или рестартирате моста, щракнете върху **Start to Reboot** (Започни рестартирането).

Щракнете върху **Save Settings** (Запис на настройките), за да приложите промените си, или щракнете върху **Cancel Changes** (Отмяна на промените), за да отмените промените си.

Administration (Администриране) > Factory Defaults (Фабрични настройки)

Чрез този екран конфигурацията на моста може да се възстанови до фабричните й настройки.

Factory Defaults (Фабрични настройки)

Restore All Settings (Възстановяване на всички настройки) За да възстановите настройките на моста до фабричните, щракнете върху **Restore All Settings** (Възстановяване на всички настройки). При възстановяване на фабричните настройки всички записани от вас настройки ще бъдат загубени.



Administration (Администриране) > Upgrade Firmware (Надстройка на фърмуер)

Чрез този екран може да се извърши надстройка на фърмуера на моста. Не се препоръчва да извършвате надстройка на фърмуера, освен ако не срещате проблеми с моста или пък ако искате да използвате функция на новия фърмуер.



Преди да извършите надстройка на фърмуера, изтеглете съответния файл за надстройка на фърмуера от уеб сайта на Linksys, **www.Linksys.com/support**.

Upgrade Firmware (Надстройка на фърмуер)

Please select a file to upgrade the firmware (Избор на файл за надстройка на фърмуера) Щракнете върху **Browse** (Преглед) и изберете файла за надстройка на фърмуера. След това щракнете върху **Start to Upgrade** (Започни надстройката) и следвайте инструкциите на екрана.

Status (Състояние) > Bridge (Мост)

Показва се информация за текущото състояние на моста.



Bridge Information (Информация за моста)

Firmware Version (Версия на фърмуера) Показва се текущата версия на фърмуера на моста.

Local Network (Локална мрежа)

Local MAC Address (Локален MAC адрес) Показва се MAC адресът на моста така, както се вижда във вашата локална Ethernet мрежа.

IP Address (IP адрес) Показва се IP адресът на моста така, както се вижда във вашата локална Ethernet мрежа.

Subnet Mask (Подмрежова маска) Показва се подмрежовата маска така, както е конфигурирана за вашата локална мрежа.

Status (Състояние) > Wireless (Безжична мрежа)

Показва се информация за вашата безжична мрежа.



Wireless (Безжична мрежа)

Link Status (Състояние на връзката) Показва се състоянието на връзката към вашата безжична мрежа.

MAC Address (MAC адрес) Показва се MAC адресът на моста така, както се вижда във вашата локална мрежа.

Network Name (SSID) (Име на мрежата - SSID) Показва се името на безжичната мрежа (SSID).

BSSID Показва се безжичният MAC адрес на свързания безжичен рутер (точка за достъп).

Radio Band (Радио обхват) Показва се радио обхватът на вашата безжична мрежа.

Channel Width (Ширина на канала) Показва се ширината на канала (в MHz), която се използва от вашата безжична мрежа.

Wide Channel (Широк канал) В зависимост от настройките за канал вашия мрежов рутер се показва Wide Channel (Широк канал). Ако сте избрали Wide (Широк) - 40 MHz канал за радио обхвата на рутера или като настройка за ширина на канала, това ще бъде вашият основен Wireless-N канал.

Standard Channel (Стандартен канал) Показва се настройката за стандартен канал. Ако сте избрали Wide (Широк) - 40 MHz канал за радио обхвата на рутера или като настройка за ширина на канала, стандартният канал ще бъде допълнителен за Wireless-N.

Bit Rate (Скорост на предаване) Показва се скоростта на предаване.

Signal (Сигнал) Показва се силата на сигнала (в проценти). 100% е най-голямата възможна сила на сигнала; 0% най-малката възможна сила на сигнала.

Security (Защита) Показва се методът на защита на вашата безжична мрежа.

Отстраняване на неизправности

WES610N/WET610N

Вашият компютър или друго кабелно Ethernet устройство не може да осъществи връзка с безжичния рутер.

1. Отворете базираната на браузър помощна програма на моста.
2. На екрана *Basic Wireless Settings* (Основни безжични настройки) проверете дали името на мрежата Network Name (SSID) съответства на името на вашата безжична мрежа.
3. Проверете дали настройките за защита (WPA, WPA2 или WEP) съответстват на настройките за защита на вашата безжична мрежа.

IP адресът на моста трябва да се смени.

Ако мостът е свързан към мрежа с DHCP сървър (обикновено мрежов рутер), то мостът ще получи своя IP адрес от DHCP сървъра. Ако няма DHCP сървър, мостът ще използва своя статичен IP адрес по подразбиране - **169.254.1.250**.

Ако искате мостът винаги да използва статичен IP адрес, следвайте инструкциите по-долу:

1. Отворете базираната на браузър помощна програма на моста.
2. Щракнете върху раздела **Network Setup** (Настройки на мрежата).
3. От падащото меню *Network Connection Type* (Тип мрежова връзка) изберете **Static IP** (Статичен IP).
4. Попълнете полетата *Static IP Address* (Статичен IP адрес), *Subnet Mask* (Подмрежова маска) и *Default Gateway* (Шлюз по подразбиране).
5. Щракнете върху **Save Settings** (Запис на настройките).

Компютърът, който използва мост или друго кабелно Ethernet устройство не осъществява връзка с друго устройство с безжична връзка (напр. компютър или принтер).

Опитайте следното:

- Проверете дали устройството с безжична връзка е в същата мрежа както компютърът или другото кабелно Ethernet устройство, свързано към моста.
- Проверете дали се използва едно и също име на мрежата (SSID) за всички устройства в безжичната мрежа.
- Проверете дали всички устройства са в една и съща IP мрежа и дали използват съвместими IP адреси.

Базираната на браузър помощна програма не приема вашата парола.

Опитайте следното:

- Паролата различава главни и малки букви. Проверете дали използвате правилно главни и малки букви при въвеждане на паролата.
- Ако сте забравили паролата си, можете да нулирате моста до фабричните му настройки.

 Натиснете и задръжте бутона **Reset** (Нулиране) на моста за прибл. пет секунди; паролата ще се нулира до фабрично настроената, **admin**. Всички други настройки на моста ще се нулират до фабричните. (За да имате достъп до базираната на браузър помощна програма, въведете **admin** в полето *Password* (Парола).)

След въвеждане на промените чрез базираната на браузър помощна програма новите настройки не се показват на екрана.

Във вашия уеб браузър щракнете върху **Refresh** (Обновяване). Ако новите настройки не се показват, следвайте инструкциите по-долу:

1. Изключете адаптера за захранване от моста.
2. Изчакайте пет секунди и след това отново го включете в моста.
3. Във вашия уеб браузър щракнете върху **Refresh** (Обновяване).

УЕБ
Ако не намирате отговори на вашите въпроси тук, направете справка в уебсайта на Linksys на адрес **Linksys.com/support**.

Спецификации

WES610N

Модел	WES610N
Стандарти	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Светодиоди	Захранване, Ethernet, Wi-Fi Protected Setup™, Безжична мрежа, отделна Ethernet връзка и активност
Портове	Ethernet (4), Захранване
Бутони	Нулиране, Wi-Fi Protected Setup
Тип кабели	CAT5e
Антени	3 (вътрешни)
Тип антенен съединител	Няма
Отделящ се (Да/Не)	Не
Модулации	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	802.11a: 15 dBm (обикновено) @ 54 Mbps 802.11b: 19 dBm (обикновено) @ 11 Mbps 802.11g: 16 dBm (обикновено) @ 54 Mbps 802.11n (2.4 GHz): 18 dBm (обикновено) @ MCS15 802.11n (5 GHz): 16 dBm (обикновено) @ MCS15
Чувствителност на приемане	802.11a: -72 dBm (обикновено) @ 54 Mbps 802.11b: -85 dBm (обикновено) @ 11 Mbps 802.11g: -73 dBm (обикновено) @ 54 Mbps 802.11n (20 MHz): -75 dBm (обикновено) @ MCS15 802.11n (40 MHz): -69 dBm (обикновено) @ MCS15
Усилване на антената в dBi	1
Защита на безжична мрежа	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Битове на защитния ключ	До 128-битово шифроване

Данни по отношение на околната среда

Размери	6.97" x 5.04" x 2.68" (177 x 128 x 68 mm)
Тегло	0.65 lb (295 g)
Сертификация	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Захранване	12 V, 1 A
Работна температура	32 до 104°F (0 до 40°C)
Температура на съхранение	-4 до 140°F (-20 до 60°C)
Работна влажност	10 до 85% без кондензация
Влажност на съхранение	5 до 90% без кондензация

Спецификациите подлежат на промени без предизвестие.

WET610N

Модел	WET610N
Стандарти	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Светодиоди	Захранване, Ethernet, Wi-Fi Protected Setup™, Wireless
Портове	Ethernet (4), Захранване
Бутони	Нулиране, Wi-Fi Protected Setup
Тип кабели	CAT5e
Антени	3 (вътрешни)
Тип антенен съединител	Няма
Отделящ се (Да/Не)	Не
Модулации	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	802.11a: 15 dBm (обикновено) @ 54 Mbps 802.11b: 18 dBm (обикновено) @ 11 Mbps 802.11g: 16 dBm (обикновено) @ 54 Mbps 802.11n: 12 dBm (обикновено) @ 130 Mbps (HT20), 270 Mbps (HT40)
Чувствителност на приемане	802.11a: -72 dBm (обикновено) @ 54 Mbps 802.11b: -85 dBm (typical) @ 11 Mbps 802.11g: -73 dBm (обикновено) @ 54 Mbps 802.11n: -70 dBm (обикновено) @ MCS15/2.4 GHz, -69 dBm (typical) @ MCS15/5.0 GHz
Усилване на антената в dBi	1
Защита на безжична мрежа	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Битове на защитния ключ	До 128-битово шифроване

Данни по отношение на околната среда

Размери	5.71" x 4.17" x 2.05" (145 x 106 x 52 mm)
Тегло	5.61 oz (159 g)
Сертификация	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Захранване	12 V, 1 A
Работна температура	32 до 104°F (0 до 40°C)
Температура на съхранение	-4 до 140°F (-20 до 60°C)
Работна влажност	10 до 85% без кондензация
Влажност на съхранение	5 до 90% без кондензация

Спецификациите подлежат на промени без предизвестие.

Linksys.com/support

Cisco, емблемата на Cisco и Linksys са търговски марки или регистрирани търговски марки на Cisco и/или неговите филиали в Съединените щати и други държави.
Списък на търговските марки на Cisco's може да се намери на адрес www.cisco.com/go/trademarks. Всички други търговски марки, упоменати в този документ, са собственост на съответните им притежатели.

© 2011 Cisco и/или неговите филиали. Всички права запазени.

3425-01249



Uživatelská příručka

Linksys WET610N/WES610N | Dvoupásmový zábavní síťový most typu N

Obsah

Přehled výrobku

Panel kontrolek LED 2
Porty 3

Důležité součásti zabezpečení bezdrátové sítě

Změna výchozího názvu nebo SSID bezdrátové sítě 4
Změna výchozího hesla 4
Aktivace filtrování podle adresy MAC 4
Aktivace šifrování 4

Obecná pravidla zabezpečení sítě 4
Další bezpečnostní tipy. 5

Pokročilé nastavení

Jak získat přístup k nástroji pro nastavení v prohlížeči 6
Setup (Nastavení) > Basic Setup (Základní nastavení) 7
Language (Jazyk) 7
Network Setup (Nastavení sítě) 7

Wireless (Bezdrátové připojení) > Basic Wireless Settings (Základní bezdrátová nastavení) 7
Basic Wireless Settings (Základní bezdrátová nastavení) 8
Wireless Security (Zabezpečení bezdrátového připojení) 8
Wi-Fi Protected Setup 9

Wireless (Bezdrátové připojení) > Wireless Network Site Survey (Přehled bezdrátových sítí) 10
Wireless Network Site Survey (Přehled bezdrátových sítí) 10

Wireless (Bezdrátové připojení) > WMM® 11
WMM 12

Wireless (Bezdrátové připojení) > Advanced Wireless Settings (Pokročilá bezdrátová nastavení) 13
Advanced Wireless (Pokročilá bezdrátová nastavení) 14

Administration (Správa) > Management (Řízení). 14
Management (Řízení) 14

Administration (Správa) > Factory Defaults (Výchozí tovární nastavení) 15
Factory Defaults (Výchozí tovární nastavení) 15

Administration (Správa) > Upgrade Firmware (Aktualizace firmwaru) 15
Upgrade Firmware (Aktualizace firmwaru) 15

Status (Stav) > Bridge (Síťový most) 15
Bridge Information (Informace o síťovém mostu) 16
Local Network (Místní síť) 16

Status (Stav) > Wireless (Bezdrátové připojení) 16
Wireless (Bezdrátové připojení) 16

Odstraňování potíží

WES610N/WET610N 17

Technické údaje

WES610N 18
WET610N 19

Přehled výrobku

Děkujeme, že jste si vybrali dvoupásmový zábavní síťový most Linksys typu N. Síťový most zajišťuje připojení síťových zařízení s pevným připojením k bezdrátové síti. Síťový most používá dvoupásmovou technologii Wireless-N a je díky tomu kompatibilní se všemi současnými technologiemi pro sítě Wi-Fi používanými bezdrátovými směrovači a přístupovými body (Wireless-N, -G, -A nebo -B). Při prvotní instalaci postupujte podle pokynů na disku CD. Ke konfiguraci pokročilých nastavení použijte nástroj pro nastavení v prohlížeči.

Panel kontrolek LED



WES610N WET610N

Bezdrátová síť (modrá) Tato kontrolka LED se rozsvítí při připojení k bezdrátové síti. Kontrolka LED bliká, když síťový most aktivně vysílá nebo přijímá data bezdrátové sítě.

Tlačítko funkce Wi-Fi Protected Setup Pokud směrovač podporuje funkci Wi-Fi Protected Setup a používá zabezpečení WPA nebo WPA2, můžete použít funkci Wi-Fi Protected Setup k automatické konfiguraci připojení síťového mostu. Informace o použití funkce Wi-Fi Protected Setup naleznete v části „Wireless (Bezdrátové připojení) > Basic Wireless Settings (Základní bezdrátová nastavení)“ na straně 7.

Kontrolka LED funkce Wi-Fi Protected Setup (modrá/žlutá) Tato kontrolka LED bliká modře po dobu dvou minut při aktivaci funkce Wi-Fi Protected Setup. Po dokončení nastavení bude modře svítit. Pokud v průběhu nastavení pomocí funkce Wi-Fi Protected Setup dojde k chybě, rozsvítí se kontrolka LED žlutě. Při použití této funkce se ujistěte, že síťový směrovač podporuje funkci Wi-Fi Protected Setup. V případě chyby vyčkejte na zhasnutí kontrolky LED a použijte funkci znovu.

Síť Ethernet (modrá) Tato kontrolka LED se rozsvítí při připojení k pevné síti. Kontrolka LED bliká, když síťový most aktivně vysílá nebo přijímá data přes pevnou síť Ethernet.

Napájení (modrá) Kontrolka LED napájení se rozsvítí po zapnutí zařízení.

Porty



WES610N WET610N

Síť Ethernet Porty sítě Ethernet zajišťují připojení síťového mostu k počítači nebo jinému zařízení s pevným připojením sítě Ethernet. Zařízení WES610N je vybaveno čtyřmi síťovými porty, zařízení WET610N má jeden port.

Reset Zařízení je možné resetovat na výchozí tovární nastavení dvěma způsoby. Buď stiskněte na přibližně pět sekund tlačítko Reset nebo obnovte výchozí nastavení v nabídce Administration (Správa) > Factory Defaults (Tovární nastavení) nástroje pro nastavení v prohlížeči. Zařízení WES610N má umístěno tlačítko pro resetování na spodní straně, zařízení WET610N jej má umístěno na zadním panelu s porty.

Napájení Prostřednictvím portu Napájení se připojuje k síťovému mostu dodávaný napájecí adaptér.

Důležité součásti zabezpečení bezdrátové sítě

Bezdrátové připojení představuje snadný a pohodlný způsob vysokorychlostního připojení k domácí síti a je v současnosti velmi rozšířené. Protože bezdrátové sítě využívají k přenosu dat rádiové vlny, jsou tyto sítě více náchylné k napadení než tradiční pevné sítě. Stejně jako komunikace mobilního nebo bezdrátového telefonu, je možné bezdrátové sítě odposlouchávat. Protože není možné fyzicky zabránit přístupu k bezdrátové síti, je potřeba podniknout zvláštní kroky k zajištění bezpečnosti sítě.

Změna výchozího názvu nebo SSID bezdrátové sítě

Bezdrátová zařízení mají z výroby nastaven výchozí název sítě, který se také označuje jako identifikátor SSID (Service Set Identifier). Název bezdrátové sítě může obsahovat až 32 znaků. Výchozí název bezdrátové sítě pro bezdrátová zařízení Linksys je **linksys**. Doporučujeme název bezdrátové sítě změnit na jedinečný název, který odliší vaši síť od ostatních bezdrátových sítí v okolí. Jako název však nepoužívejte osobní údaje (například rodné číslo), protože tyto informace budou volně dostupné každému, kdo si bude prohlížet přehled sítí.

Změna výchozího hesla

Pokud budete chtít změnit nastavení bezdrátových zařízení, jako jsou směrovače nebo přístupové body, budete vyzváni k zadání hesla. Tato zařízení mají z výroby nastaveno výchozí heslo. Výchozí heslo zařízení Linksys je **admin**. Protože jsou tyto výchozí přihlašovací údaje známy, hrozí při jejich použití, že s jejich pomocí může neoprávněná osoba snadno získat přístup k bezdrátovému zařízení a změnit nastavení sítě. Aby se takovému nebezpečí předešlo, změňte heslo zařízení tak, aby nešlo snadno uhádnout.

Aktivace filtrování podle adresy MAC

Směrovače Linksys umožňují filtrovat přístup podle adres MAC (Media Access Control) klientských zařízení. Adresa MAC je jedinečný identifikátor složený z čísel a písmen, který má přiřazeno každé síťové zařízení. Když je zapnuto filtrování podle adresy MAC, je přístup k bezdrátové síti povolen pouze určitým zařízením. Můžete například povolit pouze adresy MAC počítačů u vás doma a tím zakázat přístup všem ostatním zařízením.

Aktivace šifrování

Data přenášená v bezdrátové síti je možné chránit pomocí šifrování. Metody šifrování Wi-Fi Protected Access (WPA/WPA2) a Wired Equivalent Privacy (WEP) nabízí různé úrovně zabezpečení bezdrátové komunikace.

Šifrování WPA/WPA2 poskytuje vyšší míru zabezpečení než šifrování WEP, protože metody WPA a WPA2 používají dynamické šifrovací klíče. Kvůli zajištění ochrany bezdrátově přenášených dat je třeba používat nejdokonalejší metodu šifrování, kterou síťová zařízení podporují.

WEP je starší standard šifrování, který může být jedinou dostupnou metodou šifrování u starších zařízení, která nepodporují standard WPA.

Obecná pravidla zabezpečení sítě

Zabezpečení bezdrátové sítě je zbytečné, pokud nebude dostatečně zabezpečena vlastní síť.

- Nastavte přístupové heslo u všech počítačů v síti a samostatným heslem chraňte citlivé soubory.
- Pravidelně měňte hesla.
- Používejte antivirový software a bránu firewall.
- Nepoužívejte a zakažte sdílení souborů (sítě peer-to-peer). Některé aplikace mohou spustit sdílení souborů bez souhlasu nebo vědomí uživatele.

Další bezpečnostní tipy

- Bezdrátové směrovače, přístupové body nebo brány neinstalujte v blízkosti vnějších stěn nebo oken.
- Pokud tato bezdrátová zařízení nepoužíváte, vypněte je (v noci nebo po dobu delší nepřítomnosti).
- Používejte silná hesla, která obsahují alespoň osm znaků. V heslech používejte náhodné kombinace písmen a čísel, které se nepodobají žádnému slovu ze slovníku.

Pokročilé nastavení

Po provedení instalace síťového mostu podle pokynů na disku CD bude síťový most připraven k použití. Pokud však budete chtít změnit pokročilá nastavení, je potřeba použít nástroj pro nastavení síťového mostu v prohlížeči. V této kapitole je popsána každá webová stránka nástroje a její klíčové funkce. Nástroj lze použít z webového prohlížeče spuštěného v počítači, který je připojený k síťovému mostu.

Nástroj pro nastavení v prohlížeči obsahuje tyto hlavní karty: Setup (Nastavení), Wireless (Bezdrátová síť), Administration (Správa) a Status (Stav). Po klepnutí na některou z hlavních karet se zobrazí další karty.

Jak získat přístup k nástroji pro nastavení v prohlížeči

Nástroj se používá z webového prohlížeče.

Pokud je síťový most připojen k síti se serverem DHCP (tuto funkci obvykle zastává směrovač), potom tento server DHCP síťovému mostu přidělí IP adresu. Pokud se v síti nenachází server DHCP, používá síťový most výchozí statickou IP adresu **169.254.1.250**. (Pokud jste změnili nastavení statické IP adresy síťového mostu pomocí nástroje pro nastavení v prohlížeči, používejte pro připojení k síťovému mostu tuto adresu.)

POZNÁMKA
Pokud neznáte IP adresu síťového mostu, můžete ji zjistit v tabulce klientských zařízení DHCP směrovače. (Další informace naleznete v dokumentaci ke směrovači.)

Pokud neznáte nebo nedokážete zjistit IP adresu síťového mostu, můžete pomocí kancelářské sponky přibližně na pět sekund stisknout tlačítko **Reset**, čímž zařízení resetujete. Dojde k obnovení výchozího továrního nastavení. Síťový most si vyžádá IP adresu od serveru DHCP (tuto funkci obvykle zastává směrovač). Pokud síťový most nenalezne server DHCP, nastaví se na výchozí statickou IP adresu **169.254.1.250**, kterou bude používat, dokud nerozpozná server DHCP, který mu přidělí dynamickou IP adresu.

Pokud most není přiřazen ke směrovači a používá výchozí tovární nastavení, připojte počítač k mostu pomocí síťového kabelu, aby bylo možné použít nástroj pro nastavení v prohlížeči. K tomu je potřeba nakonfigurovat připojení k síti Ethernet v počítači nastavením statické IP adresy a masky podsítě.

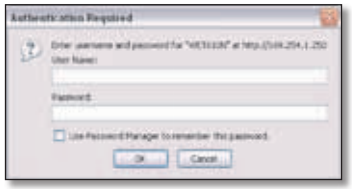
IP adresa síťového adaptéru počítače musí být nastavena podle následujících parametrů.

1. Do pole *IP address* (IP adresa) zadejte hodnotu **169.254.x.y** (x nahraďte číslem v rozsahu 1 až 254 a y číslem v rozsahu 0 až 255).
2. Do pole *Subnet mask* (Maska podsítě) zadejte hodnotu **255.255.0.0**.

POZNÁMKA
Postup nastavení statické IP adresy síťového adaptéru počítače se může lišit podle operačního systému. Pokyny naleznete v nápovědě příslušného operačního systému.

Po přiřazení statické IP adresy síťovému adaptéru počítače spusťte webový prohlížeč a zadejte IP adresu síťového mostu (výchozí hodnota je **169.254.1.250**) do *adresového řádku* prohlížeče. Stiskněte klávesu **Enter**.

Objeví se dialog pro zadání hesla. (Uživatelům, kteří používají jiný systém než Windows XP, se zobrazí podobná obrazovka.) Pole *User name* (Uživatelské jméno) nechejte prázdné. Zadejte heslo vytvořené při instalaci. Pokud jste nevytvořili nové heslo, použijte výchozí heslo **admin**. (Nové heslo můžete nastavit na obrazovce *Administration* (Správa) > *Management* (Řízení).) Pokračujte klepnutím na tlačítko **OK**.



POZNÁMKA
Pokud se dialog pro zadání hesla nezobrazí, vyčkejte dvě minuty a postup zopakujte.

Setup (Nastavení) > Basic Setup (Základní nastavení)

První obrazovka, která se zobrazí, je *Basic Setup* (Základní nastavení). Tato obrazovka umožňuje změnit jazyk nástroje pro nastavení v prohlížeči nebo změnit nastavení pevného připojení síťového mostu.





Language (Jazyk)

Language (Jazyk) Tato nabídka slouží k nastavení jazyka nástroje pro nastavení v prohlížeči. V rozevírací nabídce vyberte požadovaný jazyk.

Network Setup (Nastavení sítě)

V této části můžete určit, zda bude IP adresa síťového mostu automaticky přidělena serverem DHCP, jako je například směrovač: Automatic Configuration – DHCP (Automatická konfigurace – DHCP) nebo ručně: Static IP (Statická IP adresa).

Bridge IP (IP adresa síťového mostu) Pokud vaše síť obsahuje server DHCP (například směrovač), který přiřazuje IP adresy zařízením v síti, ponechejte výchozí nastavení **Automatic Configuration – DHCP** (Automatická konfigurace – DHCP). Síťový most si vyžádá IP adresu od serveru DHCP (tuto funkci obvykle zastává směrovač). Pokud síťový most nenalezne server DHCP, nastaví se na výchozí statickou IP adresu **169.254.1.250**, kterou bude používat, dokud nerozpozná server DHCP, který mu přidělí dynamickou IP adresu.

Pokud potřebujete síťovému mostu trvale přiřadit statickou IP adresu, vyberte možnost **Static IP** (Statická IP adresa).

Pokud vyberete možnost Static IP (Statická IP adresa), je potřeba vyplnit následující pole:

- **Static IP Address** (Statická IP adresa) Zadejte jedinečnou IP adresu, která se bude používat pro přístup k nástroji pro nastavení v prohlížeči.
- **Subnet Mask** (Maska podsítě) Zadejte masku podsítě pevné sítě.
- **Default Gateway** (Výchozí brána) Zadejte IP adresu výchozí brány sítě (většinou to je směrovač).

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Wireless (Bezdrátové připojení) > Basic Wireless Settings (Základní bezdrátová nastavení)

Pomocí obrazovky *Basic Wireless Settings* (Základní bezdrátová nastavení) nakonfigurujte základní nastavení a zabezpečení bezdrátové sítě.

Nastavení bezdrátové sítě lze nakonfigurovat ručně nebo pomocí funkce Wi-Fi Protected Setup. Wi-Fi Protected Setup je funkce, která usnadňuje nastavení bezdrátové sítě. Pokud směrovač podporuje funkci Wi-Fi Protected Setup a používá zabezpečení WPA nebo WPA2, můžete použít funkci Wi-Fi Protected Setup k automatické konfiguraci připojení síťového mostu.

Configuration View (Zobrazení konfigurace) Pokud chcete nastavení bezdrátové sítě konfigurovat ručně, zvolte možnost **Manual** (Ruční). Viz **Basic Wireless Settings** (Základní bezdrátová nastavení), **strana 8**. Pokud chcete použít funkci Wi-Fi Protected Setup, zvolte možnost **Wi-Fi Protected Setup**. Viz **Wi-Fi Protected Setup**, **strana 9**.

Basic Wireless Settings (Základní bezdrátová nastavení)



Network Name (SSID) (Název sítě (SSID)) SSID je název sítě společný pro všechna zařízení v bezdrátové síti. Všechna zařízení v bezdrátové síti musí používat stejný identifikátor SSID. Identifikátor smí obsahovat nejvýše 32 znaků, přičemž je povoleno používat libovolné znaky a rozlišuje se velikost písmen. Toto nastavení musí odpovídat nastavení bezdrátového směrovače, případně přístupového bodu. Z bezpečnostních důvodů se doporučuje změnit výchozí identifikátor SSID (**linksys**) na vlastní jedinečný název.

Wireless Security (Zabezpečení bezdrátového připojení)

Síťový most podporuje následující volby bezdrátového zabezpečení: WPA Personal, WPA2 Personal a WEP. Metody zabezpečení WPA (Wi-Fi Protected Access) a WPA2 poskytují účinnější zabezpečení než metoda WEP (Wired Equivalent Privacy). Další informace o zabezpečení bezdrátové sítě najdete v části „Důležité součásti zabezpečení bezdrátové sítě“, strana 4.

Security Mode (Režim zabezpečení)

Vyberte metodu zabezpečení pro bezdrátovou síť. Pokud nechcete používat zabezpečení bezdrátové sítě, ponechte výchozí nastavení **Disabled** (Vypnuto).

POZNÁMKA
Mějte na paměti, že všechna zařízení v bezdrátové síti MUSÍ používat stejný způsob zabezpečení a heslo nebo klíč, jinak bezdrátová zařízení nebudou schopna vzájemně komunikovat.

WPA Personal

WPA je standard zabezpečení se silnějším šifrováním, než jaké poskytuje zabezpečení WEP.



Encryption (Šifrování) Zabezpečení WPA podporuje šifrování TKIP, které používá dynamické šifrovací klíče.

Passphrase (Přístupové heslo) Zadejte klíč sdílený mezi síťovým mostem a bezdrátovým směrovačem nebo přístupovým bodem. Heslo musí obsahovat 8 až 63 znaků.

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

WPA2 Personal

WPA2 je pokročilejší verzí zabezpečení WPA, oproti kterému poskytuje vyšší úroveň zabezpečení.



Encryption (Šifrování) Zabezpečení WPA2 podporuje šifrování TKIP a AES s využitím dynamických šifrovacích klíčů. Vyberte způsob šifrování **AES** nebo **TKIP or AES** (TKIP nebo AES). Výchozí nastavení je **AES**.

Passphrase (Přístupové heslo) Zadejte klíč sdílený mezi síťovým mostem a bezdrátovým směrovačem nebo přístupovým bodem. Heslo musí obsahovat 8 až 63 znaků.

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

WEP

WEP je základní způsob šifrování, který není tak bezpečný jako zabezpečení WPA nebo WPA2.



Encryption (Šifrování) Zvolte úroveň šifrování WEP, **40/64 bit (10 hex digits)** (40/64bitové (10 hexadecimálních číslic)) nebo **104/128 bit (26 hex digits)** (104/128bitové (26 hexadecimálních číslic)). Výchozí nastavení je **40/64 bit (10 hex digits)** (40/64bitové (10 hexadecimálních číslic)).

Key 1 (Klíč 1) Zadejte bezpečnostní klíč WEP vaší sítě.

Tx Key (Klíč Tx) Síťový most používá **Key 1** (Klíč 1) jako přenosový klíč.

Authentication (Ověření) Výchozí nastavení je **Auto** (Automaticky). Při tomto nastavení je možné vybrat mezi systémem Open (Otevřené ověřování) nebo Shared (Sdílený klíč). Možnost **Open** (Otevřené ověřování) zvolte, pokud chcete používat otevřený systém ověřování, kdy odesílatel ani příjemce nepoužívají k ověření klíč WEP. Možnost **Shared** (Sdílený klíč) zvolte, pokud chcete, aby odesílatel i příjemce používali k ověřování sdílený klíč WEP.

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Wi-Fi Protected Setup

K dispozici jsou dva způsoby. Použijte způsob, který je vhodný pro váš směrovač.





Způsob č. 1

Tento způsob použijte, pokud je směrovač vybaven tlačítkem Wi-Fi Protected Setup.

1. Stiskněte tlačítko **Wi-Fi Protected Setup** na směrovači.
2. Do dvou minut potom klepněte na tlačítko **Wi-Fi Protected Setup** na obrazovce *Wi-Fi Protected Setup* síťového mostu.
3. Po nakonfigurování síťového mostu klepněte na tlačítko **Close** (Zavřít).

Na obrazovce *Wi-Fi Protected Setup* se zobrazí možnosti Link Status (Stav připojení), Network Name (SSID) (Název sítě (SSID)) a Security method (Způsob zabezpečení).

Způsob č. 2

Tento způsob použijte, pokud směrovač vyžaduje kód PIN síťového mostu.

1. Na obrazovce *Wi-Fi Protected Setup* **směrovače** zadejte kód PIN z obrazovky *Wi-Fi Protected Setup* **síťového mostu**. Potom klepněte na tlačítko **Register** (Registrovat) nebo jiné odpovídající tlačítko. (Kód je také uveden na štítku na spodní straně síťového mostu.)
2. Na obrazovce *Wi-Fi Protected Setup* **síťového mostu** klepněte na tlačítko **OK**.
3. Po nakonfigurování síťového mostu klepněte na tlačítko **Close** (Zavřít).

Na obrazovce *Wi-Fi Protected Setup* se zobrazí možnosti Link Status (Stav připojení), Network Name (SSID) (Název sítě (SSID)) a Security method (Způsob zabezpečení).

Wireless (Bezdrátové připojení) > Wireless Network Site Survey (Přehled bezdrátových sítí)

Klepnutím na kartu **Wireless Network Site Survey** (Přehled bezdrátových sítí) zobrazíte přehled aktivních bezdrátových sítí. Na obrazovce *Wireless Network Site Survey* (Přehled bezdrátových sítí) se zobrazují bezdrátové sítě, které se nachází v dosahu síťového mostu.



Wireless Network Site Survey (Přehled bezdrátových sítí)

Number of Wireless Networks (Počet bezdrátových sítí) Zde se zobrazuje počet bezdrátových sítí rozpoznaných síťovým mostem.

Select (Vybrat) Chcete-li se připojit k bezdrátové síti, klepněte na možnost **Select** (Vybrat). Pak klepněte na tlačítko **Connect** (Připojit).

Wireless Network Name (Název bezdrátové sítě) Zde se zobrazuje název nebo SSID bezdrátové sítě.

GHz (Frekvence) Zde se zobrazuje vysílací pásmo bezdrátové sítě.

Signal (Signál) Zde se zobrazuje síla signálu vyjádřená v procentech. 100 % představuje nejsilnější signál, 0 % nejslabší signál.

Security (Zabezpečení) Pokud síť podporuje funkci Wi-Fi Protected Setup, zobrazuje se zde ikona Wi-Fi Protected Setup . Zde se zobrazuje způsob zabezpečení používaný bezdrátovou sítí.

Klepnutím na tlačítko **Refresh** (Aktualizovat) aktualizujete zobrazené informace.

Po zvolení sítě klepněte na tlačítko **Connect** (Připojit). Objeví se nová obrazovka. Nyní postupujte podle pokynů pro odpovídající způsob zabezpečení sítě.

WPA



Network Name (SSID) (Název sítě (SSID)) Zde se zobrazuje název vybrané bezdrátové sítě.

Security Mode (Režim zabezpečení) Automaticky je nastavena možnost WPA Personal.

Encryption (Šifrování) Zabezpečení WPA podporuje šifrování TKIP, které používá dynamické šifrovací klíče.

Passphrase (Přístupové heslo) Zadejte klíč sdílený mezi síťovým mostem a bezdrátovým směrovačem nebo přístupovým bodem. Heslo musí obsahovat 8 až 63 znaků.

Klepnutím na tlačítko **Refresh** (Aktualizovat) aktualizujete zobrazené informace.

Po nastavení zabezpečení klepněte na tlačítko **Connect** (Připojit).

WPA2



Network Name (SSID) (Název sítě (SSID)) Zde se zobrazuje název vybrané bezdrátové sítě.

Security Mode (Režim zabezpečení) Automaticky je nastavena možnost WPA2 Personal.

Encryption (Šifrování) Zabezpečení WPA2 podporuje šifrování TKIP a AES s využitím dynamických šifrovacích klíčů. Vyberte způsob šifrování **AES** nebo **TKIP or AES** (TKIP nebo AES).

Passphrase (Přístupové heslo) Zadejte klíč sdílený mezi síťovým mostem a bezdrátovým směrovačem nebo přístupovým bodem. Heslo musí obsahovat 8 až 63 znaků.

Klepnutím na tlačítko **Refresh** (Aktualizovat) aktualizujete zobrazené informace.

Po nastavení zabezpečení klepněte na tlačítko **Connect** (Připojit).

WEP



Network Name (SSID) (Název sítě (SSID)) Zde se zobrazuje název vybrané bezdrátové sítě.

Security Mode (Režim zabezpečení) Automaticky je nastavena možnost WEP.

Encryption (Šifrování) Zvolte úroveň šifrování WEP **40/64 bit (10 hex digits)** (40/60bitové (10 hexadecimálních číslic)) nebo **104/128 bits (26 hex digits)** (104/128bitové (26 hexadecimálních číslic)).

Key 1 (Klíč 1) Zadejte bezpečnostní klíč WEP vaší sítě.

Tx Key (Klíč Tx) Síťový most používá **Key 1** (Klíč 1) jako přenosový klíč.

Authentication (Ověření) Výchozí nastavení je **Auto** (Automaticky). Při tomto nastavení je možné vybrat mezi systémem Open (Otevřené ověřování) nebo Shared (Sdílený klíč). Možnost **Open** (Otevřené ověřování) zvolte, pokud chcete používat otevřený systém ověřování, kdy odesílatel ani příjemce nepoužívají k ověření klíč WEP. Možnost **Shared** (Sdílený klíč) zvolte, pokud chcete, aby odesílatel i příjemce používali k ověřování sdílený klíč WEP.

Klepnutím na tlačítko **Refresh** (Aktualizovat) aktualizujete zobrazené informace.

Po nastavení zabezpečení klepněte na tlačítko **Connect** (Připojit).

Wireless (Bezdrátové připojení) > WMM®

Konfigurace nastavení funkce Wireless MultiMedia (WMM). Funkce WMM přiděluje paketům různé úrovně priority v závislosti na typu přenášených dat s využitím čtyř režimů přístupu: Background (Na pozadí), Best Effort (Prioritní), Video (Video) nebo Voice (Hlas). Tato nastavení by měl měnit pouze zkušený správce. Nesprávné nastavení může snížit výkon bezdrátové sítě.



POZNÁMKA
Nastavení na obrazovce *WMM* by měli měnit pouze pokročilí uživatelé.

WMM

Access Mode (Režim přístupu)

Čtyřem dostupným režimům přístupu můžete přidělit různá nastavení. Vyberte režim, který chcete nakonfigurovat: **Background** (Na pozadí), **Best Effort** (Prioritní), **Video** (Video) nebo **Voice** (Hlas). Postupujte podle pokynů pro vybraný režim.

Background (Na pozadí)

Use Aggregation (Použít agregaci) Tato možnost určuje, zda přenosová vrstva MAC (Media Access Control) bude vytvářet relaci ADDBA (Add Block Acknowledgement). Výchozí nastavení je **No** (Ne). Chcete-li tuto možnost zapnout, vyberte možnost **Yes** (Ano).

Accept Aggregation (Přijmout agregaci) Tato možnost určuje, zda bude vrstva MAC přijímat požadavky na relaci ADDBA. Výchozí nastavení je **Yes** (Ano). Chcete-li tuto možnost vypnout, vyberte nastavení **No** (Ne).

Max. Number of Packets in Aggregation (Maximální počet paketů v agregaci) Tato možnost určuje maximální počet paketů (dílčích rámců) v agregaci. Hodnota může být v rozsahu **0** až **7**. Výchozí nastavení je **7**.

Max. Aggregation Size (Maximální velikost agregace) Tato možnost určuje maximální velikost agregace (v bajtech). Hodnota může být v rozsahu **0** až **16 000**. Výchozí nastavení je **12 000**.

Timeout Internal (Interní doba platnosti) Tato možnost určuje dobu platnosti, v jejímž průběhu musí být agregace ukončena ukončující podmínkou předtím, než bude ukončena vypršením její platnost. Hodnota může být v rozsahu **0** až **100** ms. Výchozí nastavení je **3**.

Min. Size of Packet in Aggregation (Minimální velikost paketu v agregaci) Tato možnost určuje minimální velikost agregovaných paketů v bajtech. Hodnota může být v rozsahu **0** až **1 500**. Výchozí nastavení je **10**.

ADDBA Timeout (Doba platnosti relace ADDBA) Tato možnost určuje dobu, po jejímž uplynutí bude relace ADDBA ukončena, pokud během této doby neproběhne žádná výměna rámců s potvrzením přenosu bloků (ACK). Hodnota může být v rozsahu **0** až **65 535** ms. Výchozí hodnota je **0**, což znamená vypnuto.

Aggregation Window Size (Velikost okna agregace) Tato možnost určuje maximální počet paketů přenášených bez potvrzení (ACK). Hodnota může být v rozsahu **0** až **64**. Výchozí nastavení je **64**.

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Best Effort (Prioritní)

Use Aggregation (Použít agregaci) Tato možnost určuje, zda přenosová vrstva MAC (Media Access Control) bude vytvářet relaci ADDBA (Add Block Acknowledgement). Výchozí nastavení je **Yes** (Ano). Chcete-li tuto možnost vypnout, vyberte nastavení **No** (Ne).

Accept Aggregation (Přijmout agregaci) Tato možnost určuje, zda bude vrstva MAC přijímat požadavky na relaci ADDBA. Výchozí nastavení je **Yes** (Ano). Chcete-li tuto možnost vypnout, vyberte nastavení **No** (Ne).

Max. Number of Packets in Aggregation (Maximální počet paketů v agregaci) Tato možnost určuje maximální počet paketů (dílčích rámců) v agregaci. Hodnota může být v rozsahu **0** až **10**. Výchozí nastavení je **10**.

Max. Aggregation Size (Maximální velikost agregace) Tato možnost určuje maximální velikost agregace (v bajtech). Hodnota může být v rozsahu **0** až **20 000**. Výchozí nastavení je **16 000**.

Timeout Internal (Interní doba platnosti) Tato možnost určuje dobu platnosti, v jejímž průběhu musí být agregace ukončena ukončující podmínkou předtím, než bude ukončena vypršením její platnost. Hodnota může být v rozsahu **0** až **100** ms. Výchozí nastavení je **3**.

Min. Size of Packet in Aggregation (Minimální velikost paketu v agregaci) Tato možnost určuje minimální velikost agregovaných paketů v bajtech. Hodnota může být v rozsahu **0** až **1 500**. Výchozí nastavení je **10**.

ADDBA Timeout (Doba platnosti relace ADDBA) Tato možnost určuje dobu, po jejímž uplynutí bude relace ADDBA ukončena, pokud během této doby neproběhne žádná výměna rámců s potvrzením přenosu bloků (ACK). Hodnota může být v rozsahu **0** až **65 535** ms. Výchozí hodnota je **0**, což znamená vypnuto.

Aggregation Window Size (Velikost okna agregace) Tato možnost určuje maximální počet paketů přenášených bez potvrzení (ACK). Hodnota může být v rozsahu **0** až **64**. Výchozí nastavení je **64**.

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Video (Video)

Use Aggregation (Použít agregaci) Tato možnost určuje, zda přenosová vrstva MAC (Media Access Control) bude vytvářet relaci ADDBA (Add Block Acknowledgement). Výchozí nastavení je **Yes** (Ano). Chcete-li tuto možnost vypnout, vyberte nastavení **No** (Ne).

Accept Aggregation (Přijmout agregaci) Tato možnost určuje, zda bude vrstva MAC přijímat požadavky na relaci ADDBA. Výchozí nastavení je **Yes** (Ano). Chcete-li tuto možnost vypnout, vyberte nastavení **No** (Ne).

Max. Number of Packets in Aggregation (Maximální počet paketů v agregaci) Tato možnost určuje maximální počet paketů (dílčích rámců) v agregaci. Hodnota může být v rozsahu **0** až **7**. Výchozí nastavení je **7**.

Max. Aggregation Size (Maximální velikost agregace) Tato možnost určuje maximální velikost agregace (v bajtech). Hodnota může být v rozsahu **0** až **16 000**. Výchozí nastavení je **12 000**.

Timeout Internal (Interní doba platnosti) Tato možnost určuje dobu platnosti, v jejímž průběhu musí být agregace ukončena ukončující podmínkou předtím, než bude ukončena vypršením její platnost. Hodnota může být v rozsahu **0** až **100** ms. Výchozí nastavení je **3**.

Min. Size of Packet in Aggregation (Minimální velikost paketu v agregaci) Tato možnost určuje minimální velikost agregovaných paketů v bajtech. Hodnota může být v rozsahu **0** až **1 500**. Výchozí nastavení je **10**.

ADDBA Timeout (Doba platnosti relace ADDBA) Tato možnost určuje dobu, po jejímž uplynutí bude relace ADDBA ukončena, pokud během této doby neproběhne žádná výměna rámců s potvrzením přenosu bloků (ACK). Hodnota může být v rozsahu **0** až **65 535** ms. Výchozí hodnota je **0**, což znamená vypnuto.

Aggregation Window Size (Velikost okna agregace) Tato možnost určuje maximální počet paketů přenášených bez potvrzení (ACK). Hodnota může být v rozsahu **0** až **64**. Výchozí nastavení je **64**.

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Voice (Hlas)

Use Aggregation (Použít agregaci) Tato možnost určuje, zda přenosová vrstva MAC (Media Access Control) bude vytvářet relaci ADDBA (Add Block Acknowledgement). Výchozí nastavení je **Yes** (Ano). Chcete-li tuto možnost vypnout, vyberte nastavení **No** (Ne).

Accept Aggregation (Přijmout agregaci) Tato možnost určuje, zda bude vrstva MAC přijímat požadavky na relaci ADDBA. Výchozí nastavení je **Yes** (Ano). Chcete-li tuto možnost vypnout, vyberte nastavení **No** (Ne).

Max. Number of Packets in Aggregation (Maximální počet paketů v agregaci) Tato možnost určuje maximální počet paketů (dílčích rámců) v agregaci. Hodnota může být v rozsahu **0** až **2**. Výchozí nastavení je **2**.

Max. Aggregation Size (Maximální velikost agregace) Tato možnost určuje maximální velikost agregace (v bajtech). Hodnota může být v rozsahu **0** až **16 000**. Výchozí nastavení je **10 000**.

Timeout Internal (Interní doba platnosti) Tato možnost určuje dobu platnosti, v jejímž průběhu musí být agregace ukončena ukončující podmínkou předtím, než bude ukončena vypršením její platnost. Hodnota může být v rozsahu **0** až **100** ms. Výchozí nastavení je **10**.

Min. Size of Packet in Aggregation (Minimální velikost paketu v agregaci) Tato možnost určuje minimální velikost agregovaných paketů v bajtech. Hodnota může být v rozsahu **0** až **1 500**. Výchozí nastavení je **10**.

ADDBA Timeout (Doba platnosti relace ADDBA) Tato možnost určuje dobu, po jejímž uplynutí bude relace ADDBA ukončena, pokud během této doby neproběhne žádná výměna rámců s potvrzením přenosu bloků (ACK). Hodnota může být v rozsahu **0** až **65 535** ms. Výchozí hodnota je **0**, což znamená vypnuto.

Aggregation Window Size (Velikost okna agregace) Tato možnost určuje maximální počet paketů přenášených bez potvrzení (ACK). Hodnota může být v rozsahu **0** až **64**. Výchozí nastavení je **64**.

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Wireless (Bezdrátové připojení) > Advanced Wireless Settings (Pokročilá bezdrátová nastavení)

Konfigurace pokročilých funkcí bezdrátové sítě síťového mostu. Tato nastavení by měl měnit pouze zkušený správce. Nesprávné nastavení může snížit výkon bezdrátové sítě.



POZNÁMKA
Nastavení na obrazovce *Advanced Wireless Settings* (Pokročilá bezdrátová nastavení) by měli měnit pouze pokročilí uživatelé.

Advanced Wireless (Pokročilá bezdrátová nastavení)

Use LDPC (Používat LDPC) Kódování LDPC (Low-Density Parity-Check) zajišťuje opravu chyb. Při jeho použití se snižuje pravděpodobnost ztrátového přenosu dat v případě kanálů s vysokou mírou rušení. Kódování LDPC je automaticky deaktivováno algoritmem pro adaptaci přenosové rychlosti při rychlostech fyzické vrstvy (PHY) vyšších než 162. Pokud chcete povolit kódování LDPC, ponechte výchozí nastavení **Yes** (Ano). V opačném případě zvolte možnost **No** (Ne).

ERP Protection Type (Typ ochrany ERP) Tato možnost vynutí konfiguraci ochrany paketů OFDM i přes přítomnost zařízení používajících standard 802.11b. Odesláním paketů RTS/CTS nebo CTS2Self na frekvencích standardu 802.11b síťový most informuje zařízení v bezdrátové síti, že bude přenášet pakety OFDM a bude chránit přenos těchto paketů. Pakety RTS/CTS a CTS2Self zvyšují režii přenosu a mohou ve výsledku snížit přenosové rychlosti.

Možnost RTS/CTS poskytuje lepší pokrytí, ale nižší přenosové rychlosti v porovnání s možností CTS2Self, protože zahrnuje potvrzování od přijímajícího zařízení. Pokud chcete použít možnost RTS/CTS, ponechte výchozí nastavení **RTS/CTS**. Možnost None (Žádné) může způsobit kolize mezi pakety OFDM a CCK. Nechcete-li použít žádnou možnost, zvolte nastavení **None** (Žádné). Chcete-li použít možnost CTS2Self, zvolte nastavení **CTS2Self**.

11n Protection Type (Typ ochrany sítě 11n) Tato možnost nastavuje ochranu před zařízeními s nízkou přenosovou rychlostí. V případě, že bezdrátový směrovač (nebo přístupový bod) rozpozná připojení staršího zařízení s nízkou přenosovou rychlostí, signalizuje všem zařízením s vysokou přenosovou rychlostí, aby při přenosech dat používala pakety RTS/CTS nebo CTS2Self. Tato funkce podporuje všechny standardní ochranné funkce sítě 802.11n, a to včetně funkce MIMO.

Možnost RTS/CTS poskytuje lepší pokrytí, ale nižší přenosové rychlosti v porovnání s možností CTS2Self, protože zahrnuje potvrzování od přijímajícího zařízení. Pokud chcete použít možnost RTS/CTS, ponechte výchozí nastavení **RTS/CTS**. Možnost None (Žádné) může způsobit kolize mezi pakety vysokorychlostních a starších zařízení. Nechcete-li použít žádnou možnost, zvolte nastavení **None** (Žádné). Chcete-li použít možnost CTS2Self, zvolte nastavení **CTS2Self**.

Percentage of maximal transmit power (Procentuální hodnota maximálního výkonu) Tato možnost umožňuje omezit přenosový výkon nastavením procentní hodnoty maximálního výkonu odvozeného od místního omezení. Pokud bude například nejvyšší povolený místní přenosový výkon 20 dB, při zvolení hodnoty 50% se nastaví maximální výkon na 10 dB. Vyberte procentní hodnotu, kterou chcete použít: **12%**, **25%**, **50%** nebo **100%**. Výchozí nastavení je **100%**.

QoS Classification Type (Typ klasifikace QoS) Zde je možné nastavit standard 802.1D nebo 802.1Q pro mapování pole IP DSCP/TOS na priority funkce WMM (Background (Na pozadí), Best Effort (Prioritní), Video (Video), Voice (Hlas)). Ponechejte výchozí nastavení **802.1D**, případně vyberte možnost **802.1Q**, kterou používají některé datové proudy vysílání IPTV.

Re-establish Ethernet connection when initiating wireless connection (Při navázání bezdrátového připojení obnovit připojení k pevné síti) Aby se vynutilo vyhledávání serveru DHCP ze strany zařízení za síťovým mostem, síťový most obnoví ethernetové připojení mezi sebou a zařízením při každém navázání bezdrátového připojení. Chcete-li tuto funkci zakázat, vyberte možnost **No** (Ne). V opačném případě ponechejte výchozí hodnotu **Yes** (Ano).

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Administration (Správa) > Management (Řízení)

Tato obrazovka obsahuje specifické funkce a nastavení síťového mostu: nastavení přístupu k nástroji pro nastavení v prohlížeči, zálohování souboru konfigurace a restartování.



Management (Řízení)

Bridge Access (Přístup k síťovému mostu)

Umožňuje nastavit heslo pro přístup k nástroji pro nastavení v prohlížeči.

Bridge Password (Heslo síťového mostu) Zadejte nové heslo pro síťový most.

Re-enter to confirm (Opětovné zadání hesla) Zadejte heslo znovu, abyste je potvrdili.

Idle Timeout (Doba nečinnosti) Určete dobu nečinnosti, po jejímž uplynutí dojde k odhlášení uživatele. Hodnota může být v rozsahu **60** až **3 600** sekund. Výchozí nastavení je **600**.

Web Access (Přístup k webu)

Access via Wireless (Bezdrátový přístup) Pokud síťový most používáte v prostředí, kde je poskytován přístup k bezdrátové síti více osobám, můžete zakázat přístup do nástroje pro nastavení v prohlížeči prostřednictvím bezdrátového připojení. Pokud bude bezdrátový přístup zakázán, bude možné k nástroji pro nastavení v prohlížeči přistupovat pouze s využitím pevného připojení. Ponechejte výchozí nastavení **Enabled** (Povoleno), pokud chcete povolit bezdrátový přístup k nástroji pro nastavení v prohlížeči, nebo vyberte možnost **Disabled** (Zakázáno), jestliže chcete bezdrátový přístup k tomuto nástroji blokovat.

Backup (Zálohovat) a Restore (Obnovit)

Backup (Zálohovat) Chcete-li zálohovat soubor konfigurace síťového mostu, klepněte na možnost **Backup Configurations** (Zálohovat konfigurace). Potom postupujte podle pokynů na obrazovce.

Restore (Obnovit) Klepněte na tlačítko **Browse** (Procházet) a vyberte soubor konfigurace. Pak klepněte na tlačítko **Restore Configurations** (Obnovit konfigurace).

System Reboot (Restartování systému)

Reboot (Restartovat) Chcete-li zařízení restartovat, klepněte na tlačítko **Start to Reboot** (Zahájit restart).

Klepnutím na tlačítko **Save Settings** (Uložit nastavení) provedené změny použijete. Klepnutím na tlačítko **Cancel Changes** (Zrušit změny) provedené změny zrušíte.

Administration (Správa) > Factory Defaults (Výchozí tovární nastavení)

Tato obrazovka umožňuje obnovit konfiguraci síťového mostu na výchozí tovární nastavení.

Factory Defaults (Výchozí tovární nastavení)

Restore All Settings (Obnovit všechna nastavení) Chcete-li obnovit všechna nastavení, klepněte na tlačítko **Restore All Settings** (Obnovit všechna nastavení). Při obnovení výchozích nastavení ztratíte všechna uložená nastavení.



Administration (Správa) > Upgrade Firmware (Aktualizace firmwaru)

Tato obrazovka umožňuje aktualizovat firmware síťového mostu. Firmware aktualizujte pouze v případě, že máte se síťovým mostem problémy nebo nový firmware obsahuje funkci, kterou chcete používat.



Před aktualizací firmwaru si stáhněte soubor s aktualizací firmwaru síťového mostu z webových stránek **www.linksys.com/support**.

Upgrade Firmware (Aktualizace firmwaru)

Please select a file to upgrade the firmware (Zvolte soubor s aktualizací firmwaru) Klepněte na tlačítko **Browse** (Procházet) a zvolte soubor s aktualizací firmwaru. Potom klepněte na tlačítko **Start to Upgrade** (Provést aktualizaci) a postupujte podle pokynů na obrazovce.

Status (Stav) > Bridge (Síťový most)

Zde se zobrazují aktuální informace o stavu síťového mostu.



Bridge Information (Informace o síťovém mostu)

Firmware Version (Verze firmwaru) Zde se zobrazuje aktuální verze firmwaru síťového mostu.

Local Network (Místní síť)

Local MAC Address (Místní adresa MAC) Zde se zobrazuje adresa MAC, kterou síťový most používá v místní ethernetové síti.

IP Address (IP adresa) Zde se zobrazuje IP adresa, kterou síťový most používá v místní ethernetové síti.

Subnet Mask (Maska podsítě) Zde se zobrazuje maska podsítě pro místní síť.

Status (Stav) > Wireless (Bezdrátové připojení)

Zde se zobrazují informace o bezdrátové síti.



Wireless (Bezdrátové připojení)

Link Status (Stav linky) Zde se zobrazuje stav připojení k bezdrátové síti.

MAC Address (Adresa MAC) Zde se zobrazuje adresa MAC, kterou síťový most používá v místní bezdrátové síti.

Network Name (SSID) (Název sítě (SSID)) Zde se zobrazuje název bezdrátové sítě (SSID).

BSSID (BSSID) Zde se zobrazuje adresa MAC připojeného bezdrátového směrovače (případně přístupového bodu).

Radio band (Vysílací frekvence) Zde se zobrazuje vysílací pásmo bezdrátové sítě.

Channel Width (Šířka kanálu) Zde se zobrazuje používaná šířka kanálu bezdrátové sítě (v MHz).

Wide Channel (Široký kanál) V závislosti na nastavení kanálu síťového směrovače se může zobrazovat možnost Wide Channel (Široký kanál). Pokud v nastavení Radio Band (Vysílací frekvence) nebo Channel Width (Šířka kanálu) zvolíte možnost Wide Channel (Široký kanál) – 40 MHz, bude se tento kanál používat jako primární kanál sítě Wireless-N.

Standard Channel (Standardní kanál) Zde se zobrazuje hodnota pro Standard Channel (Standardní kanál). Pokud v nastavení Radio Band (Vysílací frekvence) nebo Channel Width (Šířka kanálu) zvolíte možnost Wide Channel (Široký kanál) – 40 MHz, bude se kanál Standard Channel (Standardní kanál) používat jako sekundární kanál sítě Wireless-N.

Bit Rate (Přenosová rychlost) Zde se zobrazuje rychlost přenosu dat.

Signal (Signál) Zde se zobrazuje síla signálu vyjádřená v procentech. 100 % představuje nejsilnější signál, 0 % nejslabší signál.

Security (Zabezpečení) Zde se zobrazuje způsob zabezpečení bezdrátové sítě.

Odstraňování potíží

WES610N/WET610N

Počítač nebo jiné zařízení s pevným připojením k síti Ethernet nemůže komunikovat s bezdrátovým směrovačem.

1. Spusťte nástroj pro nastavení v prohlížeči.
2. Na obrazovce *Basic Wireless Settings* (Základní bezdrátová nastavení) se ujistěte, že položka Network Name (SSID) (Název sítě (SSID)) odpovídá názvu bezdrátové sítě.
3. Ujistěte se, že nastavení zabezpečení (WPA, WPA2 nebo WEP) odpovídají nastavení zabezpečení bezdrátové sítě.

Potřebujete změnit nastavení IP adresy síťového mostu.

Pokud je síťový most připojen k síti se serverem DHCP (tuto funkci obvykle zastává směrovač), potom tento server DHCP síťovému mostu přidělí IP adresu. Pokud se v síti nenachází server DHCP, používá síťový most výchozí statickou IP adresu **169.254.1.250**.

Pokud chcete, aby síťový most vždy používal statickou IP adresu, postupujte podle následujících pokynů:

1. Spusťte nástroj pro nastavení v prohlížeči.
2. Klepněte na kartu **Network Setup** (Nastavení sítě).
3. V rozevírací nabídce *Network Connection Type* (Typ připojení k bezdrátové síti) vyberte možnost **Static IP** (Statická IP adresa).
4. Vyplňte položky *Static IP Address* (Statická IP adresa), *Subnet Mask* (Maska podsítě) a *Default Gateway* (Výchozí brána).
5. Klepněte na tlačítko **Save Settings** (Uložit nastavení).

Počítač připojený prostřednictvím síťového mostu nebo jiné zařízení připojené pevným připojením nemůže komunikovat s bezdrátovými zařízeními (např. počítačem nebo tiskárnou).

Zkontrolujte následující:

- Ujistěte se, že je bezdrátové zařízení připojeno ke stejné bezdrátové síti jako počítač nebo jiné zařízení připojené pevným připojením k síťovému mostu.
- Ujistěte se, že všechna zařízení v bezdrátové síti používají stejný název sítě (SSID).
- Ujistěte se, že jsou všechna zařízení ve stejné IP síti, používají kompatibilní IP adresy.

Nástroj pro nastavení v prohlížeči nepřijímá heslo.

Zkontrolujte následující:

- U hesla se rozlišují malá a velká písmena. Ujistěte se, že při zadávání hesla řádně používáte malá a velká písmena.
- Pokud zapomenete heslo, můžete síťový most obnovit na výchozí nastavení.

 Pokud přibližně na pět sekund stisknete tlačítko **Reset** síťového mostu, obnoví se heslo na výchozí hodnotu z výroby: **admin**. Všechna ostatní nastavení se rovněž obnoví na výchozí tovární hodnoty. (Při přístupu k nástroji pro nastavení v prohlížeči do pole *Password* (Heslo) zadejte **admin**.)

Po provedení změn v nástroji pro nastavení v prohlížeči se nová nastavení nezobrazují na obrazovce.

Klepněte na tlačítko **Refresh** (Obnovit) v prohlížeči. Pokud se nová nastavení nezobrazují, postupujte následovně:

1. Odpojte od síťového mostu napájecí kabel adaptéru.
2. Počkejte pět sekund a znovu napájecí adaptér připojte.
3. Klepněte na tlačítko **Refresh** (Obnovit) v prohlížeči.

WEB
Pokud vaše dotazy nebyly zodpovězeny, navštivte webové stránky společnosti Linksys na adrese **linksys.com/support**

Technické údaje

WES610N

Model	WES610N
Standardy	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Kontrolky LED	Napájení, síť Ethernet, funkce Wi-Fi Protected Setup™, bezdrátová síť, aktivita jednotlivých portů sítě Ethernet
Porty	Ethernet (4), napájení
Tlačítka	Reset, funkce Wi-Fi Protected Setup
Typ kabeláže	CAT 5e
Antény	3 (interní)
Typ konektoru antény	–
Odpojitelné (Ano/Ne)	Ne
Modulace	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Vysílací výkon (EIRP) v dBm	802.11a: 15 dBm (typický) @ 54 Mb/s 802.11b: 19 dBm (typický) @ 11 Mb/s 802.11g: 16 dBm (typický) @ 54 Mb/s 802.11n (2,4 GHz): 18 dBm (typický) @ MCS15 802.11n (5 GHz): 16 dBm (typický) @ MCS15
Citlivost příjmu	802.11a: –72 dBm (typická) @ 54 Mb/s 802.11b: –85 dBm (typická) @ 11 Mb/s 802.11g: –73 dBm (typická) @ 54 Mb/s 802.11n (20 MHz): –75 dBm (typická) @ MCS15 802.11n (40 MHz): –69 dBm (typická) @ MCS15
Příjem antény v dBi	1
Zabezpečení bezdrátové sítě	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Úroveň zabezpečení	Až 128bitové šifrování

Prostředí

Rozměry	177 x 128 x 68 mm
Hmotnost	295 g
Certifikace	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/n), WPA2™, Wi-Fi Protected Setup, WMM®
Napájení	12 V, 1 A
Provozní teplota	0 až 40 °C
Skladovací teplota	–20 až 60 °C
Provozní vlhkost	10 až 85 %, bez kondenzace
Skladovací vlhkost	5 až 90 %, bez kondenzace

Technické údaje se mohou změnit bez předchozího upozornění.

WET610N

Model	WET610N
Standardy	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Indikátory	Napájení, síť Ethernet, funkce Wi-Fi Protected Setup™, bezdrátová síť
Porty	Ethernet, napájení
Tlačítka	Reset, funkce Wi-Fi Protected Setup
Typ kabeláže	CAT 5e
Antény	3 (interní)
Typ konektoru antény	–
Odpojitelné (Ano/Ne)	Ne
Modulace	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Vysílací výkon (EIRP) v dBm	802.11a: 15 dBm (typický) @ 54 Mb/s 802.11b: 18 dBm (typický) @ 11 Mb/s 802.11g: 16 dBm (typický) @ 54 Mb/s 802.11b: 12 dBm (typický) @ 130 Mb/s (HT20), 270 Mb/s (HT40)
Citlivost příjmu	802.11a: –72 dBm (typická) @ 54 Mb/s 802.11b: –85 dBm (typická) @ 11 Mb/s 802.11g: –73 dBm (typická) @ 54 Mb/s 802.11n: –70 dBm (typická) @ MCS15 / 2,4 GHz, –69 dBm (typická) @ MCS15 / 5,0 GHz
Příjem antény v dBi	1
Zabezpečení bezdrátové sítě	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Úroveň zabezpečení	Až 128bitové šifrování

Prostředí

Rozměry	145 x 106 x 52 mm
Hmotnost	159 g
Certifikace	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/n), WPA2™, Wi-Fi Protected Setup, WMM®
Napájení	12 V, 1 A
Provozní teplota	0 až 40 °C
Skladovací teplota	–20 až 60 °C
Provozní vlhkost	10 až 85 %, bez kondenzace
Skladovací vlhkost	5 až 90 %, bez kondenzace

Technické údaje se mohou změnit bez předchozího upozornění.

Linksys.com/support

Cisco, logo společnosti Cisco a Linksys jsou ochranné známky nebo registrované ochranné známky společnosti Cisco nebo jejích poboček ve Spojených státech a dalších zemích.
Seznam ochranných známek společnosti Cisco najdete na adrese www.cisco.com/go/trademarks. Všechny ochranné známky uvedené v tomto dokumentu jsou majetkem příslušných vlastníků.

© 2011 společnost Cisco a její pobočky. Všechna práva vyhrazena.

3425-01249



Benutzerhandbuch

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Inhalt

Produktübersicht

LED-Anzeigen 2
Ports-Anzeige 3

Checkliste für die Wireless-Sicherheit

Ändern des Standardnamens für das Wireless-Netzwerk (SSID) 4
Ändern des Standardpassworts 4
Aktivieren der MAC-Adressfilterung 4
Aktivieren der Verschlüsselung 4
Allgemeine Richtlinien für die Netzwerksicherheit 4
Weitere Sicherheitstipps 5

Erweiterte Konfiguration

So greifen Sie auf das browserbasierte Dienstprogramm zu . . . 6
Einrichtung > Grundlegende Einrichtung 7
Sprache 7
Netzwerkeinrichtung 7
Wireless > Grundlegende Wireless-Einstellungen 7
Grundlegende Wireless-Einstellungen 8
Wireless-Sicherheit 8
Wi-Fi Protected Setup 9
Wireless > Wireless-Netzwerksuche 10
Wireless-Netzwerksuche 10
Wireless > WMM® 11
WMM 12
Wireless > Advanced Wireless Settings (Erweiterte Wireless-Einstellungen) 13
Erweiterte Wireless-Einstellungen 14
Administration (Verwaltung) > Management (Verwaltungsfunktionen) 14
Verwaltungsfunktionen 15
Verwaltung > Werkseinstellungen 15
Werkseinstellungen 15
Verwaltung > Firmware aktualisieren 15
Firmware aktualisieren 15
Status > Bridge 16
Bridge-Informationen 16
Lokales Netzwerk 16
Status > Wireless 16
Wireless-Geräte 16

Fehlerbehebung

WES610N/WET610N 17

Spezifikationen

WES610N 18
WET610N 19

Produktübersicht

Vielen Dank, dass Sie sich für die Linksys Dual-Band N Entertainment Bridge entschieden haben. Die Bridge kann eine Verbindung mit jedem kabelgebundenen Ethernet-Gerät in Ihrem Wireless-Netzwerk herstellen. Sie basiert auf der Dual-Band Wireless-N-Technologie und ist damit kompatibel mit jedem Wireless-N-, -G-, -A- oder B-Router bzw. Access Point. Befolgen Sie für die Erstinstallation die Anweisungen auf dem CD-Faltblatt. Zur Konfiguration erweiterter Einstellungen können Sie das praktische browserbasierte Dienstprogramm verwenden.

LED-Anzeigen



WES610N WET610N

Wireless (Blau) Die Wireless-LED leuchtet, wenn eine Wireless-Verbindung besteht. Die LED blinkt, wenn die Bridge gerade Daten über das Wireless-Netzwerk sendet oder empfängt.

Wi-Fi Protected Setup Wenn Ihr Router die Wi-Fi Protected Setup-Funktion unterstützt und WPA- oder WPA2 verwendet, können Sie Wi-Fi Protected Setup für eine automatische Verbindung mit der Bridge verwenden. Informationen zur Verwendung von Wi-Fi Protected Setup finden Sie unter „Wireless > Grundlegende Wireless-Einstellungen“ auf Seite 7.

Wi-Fi Protected Setup (Blau/Orange) Die LED blinkt während des Wi-Fi Protected Setup für zwei Minuten blau Sie leuchtet blau, wenn die Wireless-Sicherheitsfunktion aktiviert ist. Wenn während des Wi-Fi Protected Setup-Prozesses ein Fehler auftritt, leuchtet die LED orange. Vergewissern Sie sich, dass der Netzwerk-Router Wi-Fi Protected Setup unterstützt. Warten Sie, bis die LED nicht mehr leuchtet, und versuchen Sie es anschließend erneut.

Ethernet (Blau) Die Ethernet-LED leuchtet, wenn eine Wireless-Verbindung besteht. Die LED blinkt, wenn die Bridge gerade Daten über den/die Ethernet-Port(s) sendet oder empfängt.

Power (Blau) Die Power-LED leuchtet, wenn die Bridge eingeschaltet ist.

Ports-Anzeige



WES610N WET610N

Ethernet Der/Die Ethernet-Port(s) verbindet/n die Bridge mit einem Computer oder einem anderen Ethernet-Netzwerkgerät. Die WES610N hat vier Ports, die WET610N hat einen Port.

Reset Die Bridge kann auf zweierlei Weise auf die Werkseinstellungen zurückgesetzt werden. Halten Sie entweder die Reset-Taste ungefähr fünf Sekunden lang gedrückt, oder stellen Sie die Standardeinstellungen im webbasierten Dienstprogramm der Bridge unter Administration > Factory Defaults (Verwaltung > Werkseinstellungen) wieder her. Beim WES610N befindet sich die Reset-Taste auf der Unterseite, bei der WET610N auf der Rückseite.

Power Der Power-Port dient zum Anschließen des Netzteils an die Bridge.

Checkliste für die Wireless-Sicherheit

Wireless-Netzwerke sind praktisch und einfach zu installieren, folglich greifen immer mehr Privatanwender mit Highspeed-Internetzugriff darauf zurück. Da die Daten bei Wireless-Netzwerken per Funk übertragen werden, ist diese Art von Netzwerk anfälliger für unberechtigte Zugriffe als ein herkömmliches Kabel-Netzwerk. Wie Signale von mobilen oder kabellosen Telefonen können auch Signale aus Wireless-Netzwerken abgefangen werden. Da Sie unberechtigte Personen nicht physisch daran hindern können, eine Verbindung mit Ihrem Wireless-Netzwerk herzustellen, müssen Sie einige zusätzliche Maßnahmen zum Schutz des Netzwerks ergreifen.

Ändern des Standardnamens für das Wireless-Netzwerk (SSID)

Wireless-Geräten wird werkseitig ein Standard-Wireless-Netzwerkname bzw. eine SSID (Service Set Identifier) zugewiesen. Dies ist der Name Ihres Wireless-Netzwerks, der bis zu 32 Zeichen umfassen darf. Wireless-Produkte von Linksys verwenden **linksys** als Standardnamen für das Wireless-Netzwerk. Sie sollten den Wireless-Netzwerknamen in einen eindeutigen Namen ändern, um ihn von anderen Netzwerken zu unterscheiden, die möglicherweise in Ihrer Umgebung vorhanden sind. Verwenden Sie jedoch keine personenbezogenen Informationen (wie etwa Ihre Kontonummer), da diese Informationen bei der Suche nach Wireless-Netzwerken für jeden sichtbar sind.

Ändern des Standardpassworts

Wenn Sie die Einstellungen von Wireless-Geräten wie Access Points und Routern ändern möchten, werden Sie zur Eingabe des Passworts aufgefordert. Für diese Geräte wurde werkseitig ein Standardpasswort festgelegt. Das Standardpasswort von Linksys lautet **admin**. Hacker kennen diese Passwörter und könnten versuchen, damit auf Ihr Wireless-Gerät zuzugreifen und Ihre Netzwerkeinstellungen zu ändern. Um jegliche unberechtigten Änderungen zu verhindern, sollten Sie das Gerätepasswort so anpassen, dass es schwer zu erraten ist.

Aktivieren der MAC-Adressfilterung

Bei den Routern von Linksys können Sie die MAC-Adressfilterung (Media Access Control) aktivieren. Eine MAC-Adresse ist eine eindeutige Reihe von Nummern und Buchstaben, die dem jeweiligen Netzwerkgerät zugewiesen wird. Wenn die MAC-Adressfilterung aktiviert ist, können nur Wireless-Geräte mit bestimmten MAC-Adressen auf das Wireless-Netzwerk zugreifen. Beispielsweise können Sie die MAC-Adressen der verschiedenen Computer bei sich zu Hause angeben, sodass nur diese Computer Zugang zu Ihrem Wireless-Netzwerk haben.

Aktivieren der Verschlüsselung

Mit der Verschlüsselung werden die über ein Wireless-Netzwerk gesendeten Daten geschützt. WPA/WPA2 (Wi-Fi Protected Access), PSK (Pre-Shared Key) und WEP (Wired Equivalency Privacy) bieten verschiedene Sicherheitsstufen für die Wireless-Kommunikation.

Ein mit WPA/WPA2 verschlüsseltes Netzwerk ist sicherer als ein Netzwerk, das nur mit WEP verschlüsselt ist, weil WPA/WPA2 eine dynamische Verschlüsselung verwendet. Um Daten zu schützen, während diese per Funk übertragen werden, sollten Sie die höchste Verschlüsselungsstufe einsetzen, die von Ihren Netzwerkgeräten unterstützt wird.

Bei WEP handelt es sich um einen älteren Verschlüsselungsstandard, der eventuell auf bestimmten älteren Geräten, die WPA nicht unterstützen, die einzig verfügbare Möglichkeit ist.

Allgemeine Richtlinien für die Netzwerksicherheit

Sämtliche Sicherheitsmaßnahmen für Ihr Wireless-Netzwerk sind jedoch zwecklos, wenn das zugrunde liegende Netzwerk nicht sicher ist.

- Schützen Sie alle Computer im Netzwerk sowie vertrauliche Dateien durch Passwörter.
- Ändern Sie die Passwörter regelmäßig.
- Installieren Sie Software für den Virenschutz und eine persönliche Firewall.
- Deaktivieren Sie die Dateifreigabe für Peer-to-Peer-Netzwerke, die gemeinsam auf Dateien zugreifen. Manche Anwendungen aktivieren die Dateifreigabe möglicherweise ohne Ihr Wissen bzw. Ihre Zustimmung.

Weitere Sicherheitstipps

- Halten Sie Wireless-Geräte wie Router, Access Points oder Gateways von Außenwänden und Fenstern fern.
- Schalten Sie Wireless-Router, Access Points oder Gateways aus, wenn sie nicht genutzt werden (nachts, im Urlaub).
- Verwenden Sie sichere Passwörter, die mindestens acht Zeichen lang sind. Kombinieren Sie Zahlen und Buchstaben, um keine Standardwörter zu verwenden, die in Wörterbüchern zu finden sind.

Erweiterte Konfiguration

Nach Einrichtung der Bridge mit den im CD-Faltblatt beschriebenen Schritten ist die Bridge bereit zur Nutzung. Die erweiterten Einstellungen können Sie allerdings nur mithilfe des browserbasierten Dienstprogramms ändern. In diesem Kapitel werden alle Webseiten des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können das Dienstprogramm über einen Webbrowser auf einem Computer aufrufen, der an die Bridge angeschlossenen ist.

Das browserbasierte Dienstprogramm verfügt über diese Hauptregisterkarten: Setup (Einrichtung), Wireless, Administration (Verwaltung) und Status. Durch Klicken der Hauptregisterkarten werden zusätzliche Registerkarten verfügbar.

So greifen Sie auf das browserbasierte Dienstprogramm zu

Verwenden Sie einen Webbrowser, um auf das browserbasierte Dienstprogramm zuzugreifen.

Wenn die Bridge mit einem Netzwerk mit DHCP-Server verbunden ist (in der Regel der Netzwerk-Router), ruft die Bridge die IP-Adresse vom DHCP-Server ab. Wenn kein DHCP-Server erkannt wird, wird für die Bridge die statische Standard-IP-Adresse **169.254.1.250** verwendet. (Wenn Sie über das browserbasierte Dienstprogramm eine permanente statische IP-Adresse auf der Bridge festlegen, geben Sie stattdessen die statische IP-Adresse ein.)

HINWEIS
Wenn Sie die IP-Adresse der Bridge nicht kennen, finden Sie sie in der DHCP-Client-Tabelle Ihres Routers. (Informationen dazu finden Sie in der Dokumentation zu Ihrem Router.)

Wenn Sie die IP-Adresse der Bridge nicht finden können, können Sie die Bridge zurücksetzen. Halten Sie dazu die Taste **Reset** auf der Bridge etwa fünf Sekunden lang mithilfe einer aufgebogenen Büroklammer gedrückt. Dadurch wird die Bridge auf die Werkseinstellungen zurückgesetzt. Die Bridge fordert dann eine IP-Adresse vom DHCP-Server (in der Regel der Netzwerkrouter) an. Wird kein DHCP-Server gefunden, verwendet die Bridge ihre statische Standard-IP-Adresse **169.254.1.250**, bis sie einen DHCP-Server erkennt und ihr eine dynamische IP-Adresse zugewiesen wird.

Wenn die Bridge nicht mit einem Router verbunden ist und die standardmäßigen Werkseinstellungen verwendet werden, verbinden Sie einen Computer per Ethernet mit der Bridge, um auf das web-basierte Dienstprogramm zuzugreifen. Die Ethernet-Verbindung müssen Sie auf dem Computer mit einer statische IP-Adresse und Subnetzmaske konfigurieren.

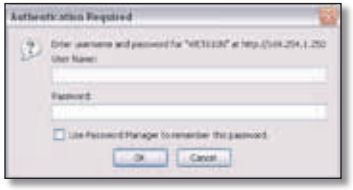
Für den Ethernet-Adapter sollte eine bestimmte IP-Adresse eingestellt sein.

1. Geben Sie im Feld *IP address* (IP-Adresse) **169.254.x.y** (x muss dabei durch eine Zahl zwischen 1 und 254, y durch eine Zahl zwischen 0 und 255 ersetzt werden) ein.
2. Geben Sie im Feld *Subnet Mask* (Subnetzmaske) **255.255.0.0** ein.

HINWEIS
Die Schritte zum Zuweisen einer statischen IP-Adresse zum Ethernet-Adapter auf dem Computer sind je nach Betriebssystem verschieden. Anweisungen dazu finden Sie in der Hilfe zu Ihrem Betriebssystem.

Wenn Sie dem Ethernet-Adapter eine statische IP-Adresse zugewiesen haben, starten Sie Ihren Webbrowser und geben die IP-Adresse des Adapters in das *Adressfeld* ein (die Standardeinstellung ist **169.254.1.250**). Drücken Sie die **Eingabetaste**.

Das Passwort-Eingabefenster wird angezeigt. (Unter anderen Betriebssystemen als Windows XP wird ein ähnliches Fenster angezeigt.) Lassen Sie das Feld *User Name* (Benutzername) leer. Geben Sie das Passwort ein, das Sie bei der Einrichtung erstellt haben. Wenn Sie kein Passwort erstellt haben, verwenden Sie das Standardkennwort **admin**. Sie können im Fenster *Administration* (Verwaltung) > *Management* (Verwaltungsfunktionen) ein neues Passwort festlegen. Klicken Sie auf **OK**, um fortzufahren.



HINWEIS
Wird das Fenster zur Passworteingabe nicht angezeigt, warten Sie zwei Minuten, und versuchen Sie es dann erneut.

Einrichtung > Grundlegende Einrichtung

Im ersten geöffneten Fenster wird die Registerkarte *Basic Setup* (Grundlegende Einrichtung) angezeigt. In diesem Fenster können Sie die Sprache des browserbasierten Dienstprogramms oder die die Einstellungen des kabelgebundenen Ethernet-Netzwerks der Bridge ändern.





Sprache

Language (Sprache) Hier können Sie die Anzeigesprache des browserbasierten Dienstprogramms festlegen. Wählen Sie im Dropdown-Menü die gewünschte Sprache aus.

Netzwerkeinrichtung

In diesem Abschnitt wird festgelegt, ob die IP-Adresse der Bridge automatisch von einem DHCP-Server, zum Beispiel einem Netzwerk-Router, abgerufen (Automatic Configuration - DHCP (Automatische Konfiguration - DHCP)) oder manuell eingerichtet wird (Static IP (Statische IP)).

Bridge IP (Bridge-IP) Wenn Ihr Netzwerk einen DHCP-Server, zum Beispiel einen Netzwerk-Router, hat, über den Ihren Netzwerkgeräten IP-Adressen zugewiesen werden, behalten Sie die Standardeinstellung **Automatic Configuration - DHCP** (Automatische Konfiguration - DHCP) bei. Die Bridge fordert dann eine IP-Adresse vom DHCP-Server (in der Regel der Netzwerkrouter) an. Wird kein DHCP-Server gefunden, verwendet die Bridge ihre statische Standard-IP-Adresse **169.254.1.250**, bis sie einen DHCP-Server erkennt und ihr eine dynamische IP-Adresse zugewiesen wird.

Wählen Sie **Static IP** (Statische IP), wenn Sie eine permanente statische IP-Adresse für die Bridge festlegen möchten.

Wenn Sie **Static IP** (Statische IP) auswählen, müssen Sie die folgenden Felder ausfüllen:

- **Static IP Address** (Statische IP-Adresse) Geben Sie eine eindeutige IP-Adresse für den Zugriff auf das browserbasierte Dienstprogramm ein.
- **Subnet Mask** (Subnetzmaske) Geben Sie die Subnetzmaske des kabelgebundenen Netzwerks ein.
- **Default Gateway** (Standard-Gateway) Geben Sie die IP-Adresse des Standard-Gateways für das Netzwerk ein (in den meisten Fällen ist das der Router).

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Wireless > Grundlegende Wireless-Einstellungen

Verwenden Sie das Fenster *Basic Wireless Settings* (Grundlegende Wireless-Einstellungen), um die grundlegenden Wireless- und Sicherheitseinstellungen der Bridge zu konfigurieren.

Es gibt zwei Möglichkeiten zur Konfiguration der Bridge-Einstellungen: manuell und mit WPS (Wi-Fi Protected Setup). Bei Wi-Fi Protected Setup handelt es sich um eine Funktion, mit der Sie auf einfache Weise das Wireless-Netzwerk einrichten können. Wenn Ihr Netzwerkrouter die Wi-Fi Protected Setup-Funktion unterstützt und WPA- oder WPA2 verwendet, können Sie Wi-Fi Protected Setup für eine automatische Verbindung der Bridge verwenden.

Configuration View (Konfigurationsansicht) Wählen Sie zur manuellen Konfiguration des Wireless-Netzwerks die Option **Manual** (Manuell). Weitere Informationen finden Sie unter **Grundlegende Wireless-Einstellungen**, **Seite 8**. Wenn Sie Wi-Fi Protected Setup verwenden möchten, wählen Sie **Wi-Fi Protected Setup**. Informationen dazu finden Sie unter **Wi-Fi Protected Setup**, **Seite 9**.

Grundlegende Wireless-Einstellungen



Network Name (SSID) (Netzwerkname, SSID) Bei der SSID (Service Set Identifier) handelt es sich um den Netzwerknamen, der von allen Punkten im Wireless-Netzwerk verwendet wird. Die SSID muss für alle Geräte im Wireless-Netzwerk identisch sein. Für die maximal 32 Zeichen lange SSID dürfen alle Zeichen der Tastatur verwendet werden. Es wird zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass diese Einstellung mit der entsprechenden Einstellung auf dem Wireless-Router oder Access Point übereinstimmt. Um die Sicherheit zu erhöhen, sollten Sie die Standard-SSID (**linksys**) in einen eindeutigen Namen ändern.

Wireless-Sicherheit

Die Bridge unterstützt die folgenden Wireless-Sicherheitsoptionen: WPA Personal, WPA2 Personal und WEP WPA (Wi-Fi Protected Access) und WPA2 sind stärkere Sicherheitsmethoden als WEP (Wired Equivalent Privacy). Weitere Informationen zur Wireless-Sicherheit finden Sie unter „Checkliste für die Wireless-Sicherheit", Seite 4.

Sicherheitsmodus

Wählen Sie die Sicherheitsmethode für Ihr Wireless-Netzwerk aus. Wenn Sie die Wireless-Sicherheit nicht verwenden möchten, behalten Sie die Standardeinstellung **Disabled** (Deaktiviert) bei.

HINWEIS
Denken Sie daran, dass jedes Gerät im Wireless-Netzwerk die gleiche Sicherheitsmethode und das gleiche Passwort/den gleichen Schlüssel verwenden MUSS. Ist dies nicht der Fall, können die Wireless-Geräte nicht miteinander kommunizieren.

WPA-Personal

WPA ist ein Sicherheitsstandard, der über die WEP-Verschlüsselung hinausgeht.



Encryption (Verschlüsselung) WPA unterstützt die Verschlüsselungsmethode TKIP mit dynamischen Verschlüsselungsschlüsseln.

Passphrase Geben Sie den von der Bridge und Ihrem Wireless-Router oder Access Point verwendeten gemeinsamen Schlüssel ein. Er muss aus 8 bis 63 Zeichen bestehen.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

WPA2-Personal

WPA2 ist eine komplexere, sicherere Version von WPA.



Encryption (Verschlüsselung) WPA2 unterstützt zwei Verschlüsselungsmethoden: TKIP und AES mit dynamischen Verschlüsselungsschlüsseln. Wählen Sie die gewünschte Verschlüsselungsmethode aus: **AES**, **TKIP oder AES**. Standardmäßig ist **AES** ausgewählt.

Passphrase Geben Sie den von der Bridge und dem Wireless-Router oder Access Point verwendeten gemeinsamen Schlüssel ein. Er muss aus 8 bis 63 Zeichen bestehen.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

WEP

WEP ist eine einfache Verschlüsselungsmethode, die nicht so sicher wie WPA oder WPA2 ist.



Encryption (Verschlüsselung) Wählen Sie eine WEP-Verschlüsselungsstufe aus: **40/64 bits (10 hex digits)** (40/64 Bit (10 Hexadezimalziffern)) oder **104/128 bits (26 hex digits)** (104/128 Bit (26 Hexadezimalziffern)). Der Standardwert ist **40/64 bits (10 hex digits)** (40/64-Bit (10 Hexadezimalziffern)).

Key 1 (Schlüssel 1) Geben Sie den WEP-Schlüssel Ihres Netzwerks ein.

Tx Key (TX-Schlüssel) **Key 1** (Schlüssel 1) ist der von der Bridge verwendete Übertragungsschlüssel.

Authentication Type (Authentifizierungstyp) Standardmäßig ist die Option **Auto** (Automatisch) ausgewählt, mit der sowohl der Authentifizierungstyp **Open System** (Offenes System) als auch **Shared Key** (Gemeinsamer Schlüssel) verwendet werden kann. Wählen Sie **Open** (Offen), wenn der Authentifizierungstyp **Offenes System** verwendet werden soll, bei dem der Absender und der Empfänger keinen WEP-Schlüssel zur Authentifizierung verwenden. Wählen Sie **Shared** (Freigegeben), wenn der Authentifizierungstyp **Gemeinsamer Schlüssel** verwendet werden soll, bei dem der Absender und der Empfänger einen WEP-Schlüssel zur Authentifizierung verwenden.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Wi-Fi Protected Setup

Sie können aus zwei Methoden auswählen. Wählen Sie die Methode, die auf den von Ihnen eingesetzten Router zutrifft.





Methode 1

Verwenden Sie diese Methode, wenn Ihr Router über eine Wi-Fi Protected Setup-Taste verfügt.

1. Drücken Sie die **Wi-Fi Protected Setup**-Taste am Router.
2. Klicken Sie innerhalb von zwei Minuten auf die Taste **Wi-Fi Protected Setup** im Fenster *Wi-Fi Protected Setup* der Bridge.
3. Nachdem die Bridge konfiguriert wurde, klicken Sie auf **Close** (Schließen).

Im Fenster *Wi-Fi Protected Setup* wird der Verbindungsstatus, Netzwerkname (SSID) und die Sicherheitsmethode angezeigt.

Methode 2

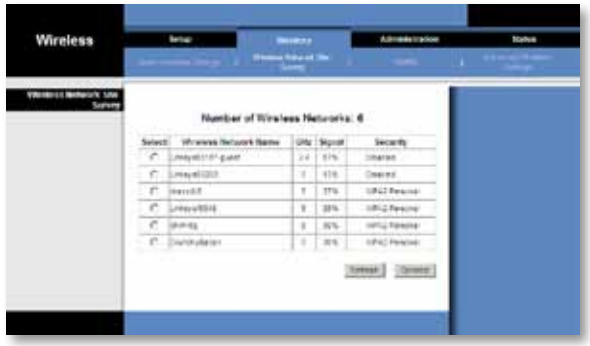
Verwenden Sie diese Methode, wenn auf dem Router die Eingabe der PIN für die Bridge erforderlich ist.

1. Geben Sie im Fenster *Wi-Fi Protected Setup* des **Routers** die PIN ein, die im Fenster *Wi-Fi Protected Setup* der **Bridge** angegeben ist. Klicken Sie anschließend auf **Register** (Registrieren) oder eine entsprechende Schaltfläche. (Die PIN ist auch auf dem Etikett an der Unterseite der Bridge angegeben.)
2. Klicken Sie im Fenster *Wi-Fi Protected Setup* der **Bridge** auf **OK**.
3. Nachdem die Bridge konfiguriert wurde, klicken Sie auf **Close** (Schließen).

Im Fenster *Wi-Fi Protected Setup* wird der Verbindungsstatus, Netzwerkname (SSID) und die Sicherheitsmethode angezeigt.

Wireless > Wireless-Netzwerksuche

Klicken Sie auf die Registerkarte **Wireless Network Site Survey** (Wireless-Netzwerksuche), um eine Netzwerksuche zu starten. In der Liste *Wireless Network Site Survey* (Wireless-Netzwerksuche) werden alle von der Bridge erkannten Wireless-Netzwerke aufgeführt.



Wireless-Netzwerksuche

Number of Wireless Networks (Anzahl der Wireless-Netzwerke) Hier wird die Zahl der von der Bridge erkannten Wireless-Netzwerke angezeigt.

Wählen Sie diese Option, um eine Verbindung zu einem Wireless-Netzwerk herzustellen, klicken Sie auf **Select** (Auswählen). Klicken Sie anschließend auf **Connect** (Verbinden).

Wireless Network Name (Wireless-Netzwerkname) Dies ist der Netzwerkname oder die SSID des angezeigten Wireless-Netzwerks.

GHz Das Frequenzband des angezeigten Wireless-Netzwerks.

Signal Hier wird der Prozentsatz der Signalstärke angezeigt. 100 % ist die höchstmögliche, 0 % die geringstmögliche Signalstärke.

Security (Sicherheit) Wenn das Netzwerk Wi-Fi Protected Setup unterstützt, wird das Symbol für Wi-Fi Protected Setup angezeigt. Hier wird die vom Wireless-Netzwerk verwendete Sicherheitsmethode angezeigt.

Klicken Sie auf **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.

Klicken Sie nach der Auswahl des Wireless-Netzwerks auf **Connect** (Verbinden). Ein neues Fenster wird angezeigt. Folgen Sie der Anleitung zum Konfigurieren der Sicherheitsmethode für das Netzwerk.

WPA



Network Name (SSID) (Netzwerkname, SSID) Der Name des gewählten Netzwerks wird automatisch angezeigt.

Security Mode (Sicherheitsmodus) WPA Personal wird automatisch angezeigt.

Encryption (Verschlüsselung) WPA unterstützt die Verschlüsselungsmethode TKIP mit dynamischen Verschlüsselungsschlüsseln.

Passphrase Geben Sie den von der Bridge und dem Wireless-Router oder Access Point verwendeten gemeinsamen Schlüssel ein. Er muss aus 8 bis 63 Zeichen bestehen.

Klicken Sie auf **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.

Klicken Sie nach der Eingabe der Sicherheitseinstellungen auf **Connect** (Verbinden).

WPA2



Network Name (SSID) (Netzwerkname, SSID) Der Name des gewählten Netzwerks wird automatisch angezeigt.

Security Mode (Sicherheitsmodus) WPA2 Personal wird automatisch angezeigt.

Encryption (Verschlüsselung) WPA2 unterstützt zwei Verschlüsselungsmethoden: TKIP und AES mit dynamischen Verschlüsselungsschlüsseln. Wählen Sie die gewünschte Verschlüsselungsmethode aus: **AES**, **TKIP oder AES**.

Passphrase Geben Sie den von der Bridge und dem Wireless-Router oder Access Point verwendeten gemeinsamen Schlüssel ein. Er muss aus 8 bis 63 Zeichen bestehen.

Klicken Sie auf **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.

Klicken Sie nach der Eingabe der Sicherheitseinstellungen auf **Connect** (Verbinden).

WEP



Network Name (SSID) (Netzwerkname, SSID) Der Name des gewählten Netzwerks wird automatisch angezeigt.

Security Mode (Sicherheitsmodus) WEP wird automatisch angezeigt.

Encryption (Verschlüsselung) Wählen Sie eine WEP-Verschlüsselungsstufe aus: **40/64 bits (10 hex digits)** (40/64 Bit (10 Hexadezimalziffern)) oder **104/128 bits (26 hex digits)** (104/128 Bit (26 Hexadezimalziffern)).

Key 1 (Schlüssel 1) Geben Sie den WEP-Schlüssel Ihres Netzwerks ein.

Tx Key (TX-Schlüssel) **Key 1** (Schlüssel 1) ist der von der Bridge verwendete Übertragungsschlüssel.

Authentication Type (Authentifizierungstyp) Standardmäßig ist die Option **Auto** (Automatisch) ausgewählt, mit der sowohl der Authentifizierungstyp **Open System** (Offenes System) als auch **Shared Key** (Gemeinsamer Schlüssel) verwendet werden kann. Wählen Sie **Open** (Offen), wenn der Authentifizierungstyp „Offenes System" verwendet werden soll, bei dem der Absender und der Empfänger keinen WEP-Schlüssel zur Authentifizierung verwenden. Wählen Sie **Shared** (Freigegeben), wenn der Authentifizierungstyp **Gemeinsamer Schlüssel** verwendet werden soll, bei dem der Absender und der Empfänger einen WEP-Schlüssel zur Authentifizierung verwenden.

Klicken Sie auf **Aktualisieren**, um die angezeigten Informationen zu aktualisieren.

Klicken Sie nach der Eingabe der Sicherheitseinstellungen auf **Connect** (Verbinden).

Wireless > WMM®

Konfigurieren Sie die Einstellungen für Wireless Multimedia (WMM). WMM weist Paketen abhängig vom jeweiligen Zugriffsmodus (Verkehrstyp) Prioritäten zu: Background (Hintergrund), Best Effort (Beste Bemühung), Video oder Voice (Sprache). Diese Einstellungen sollten nur von einem erfahrenen Administrator angepasst werden, da falsche Einstellungen die Leistung des Routers im Wireless-Betrieb beeinträchtigen können.



HINWEIS
Die Einstellungen im Fenster *WMM* sind auf fortgeschrittene Nutzer zugeschnitten.

WMM

Zugriffsmodus

Sie können den vier verfügbaren Zugriffsmodi unterschiedliche Einstellungen zuordnen. Wählen Sie den Modus aus, den Sie konfigurieren möchten: **Background** (Hintergrund), **Best Effort** (Beste Bemühung), **Video** oder **Voice** (Sprache). Befolgen Sie die Anweisungen für den gewählten Modus.

Hintergrund

Use Aggregation (Aggregation verwenden) Diese Option definiert, ob die MAC-Ebene (Media Access Control) eine ADDBA-Sitzung (Add Block Acknowledgement) einrichtet oder nicht. Die Standardeinstellung ist **No** (Nein). Wählen Sie **Yes** (Ja), um die Option zu aktivieren.

Accept Aggregation (Aggregation annehmen) Mit dieser Option wird festgelegt, ob die MAC-Ebene eine ADDBA-Anforderung annimmt oder nicht. Der Standardwert ist **Yes** (Ja). Wählen Sie **No** (Nein), um diese Option zu deaktivieren.

Max. Number of Packets in Aggregation (Max. Anzahl der Pakete in der Aggregation) Diese Option definiert die maximale Anzahl der Pakete (Sub-Frames) in einer Aggregation. Der gültige Bereich ist **0** bis **7**. Der Standardwert ist **7**.

Max. Aggregation Size (Max. Größe der Aggregation) Diese Option definiert die maximale Größe der Aggregation (in Byte). Der gültige Bereich ist **0** bis **16000**. Der Standardwert ist **12000**.

Timeout Interval (Zeitüberschreitungs-Intervall) Mit dieser Option wird das Zeitintervall festgelegt, vor dessen Ablauf die Aggregation mit einem „Abschlussstatus" geschlossen werden sollte, damit das Zeitlimit nicht überschritten wird. Der gültige Bereich ist **0** bis **100** ms. Der Standardwert ist **3**.

Size of Packet in Aggregation (Min. Größe der Pakete in der Aggregation) Diese Option definiert die minimale Größe (in Byte) der Pakete, die in der Aggregation zusammengestellt werden können. Der gültige Bereich ist **0** bis **1500**. Der Standardwert ist **10**.

ADDBA Timeout (ADDBA-Zeitüberschreitung) Mit dieser Option wird das Zeitintervall festgelegt, nach dessen Ablauf die ADDBA-Einrichtung abgebrochen wird, sofern innerhalb dieses Zeitraums keine Frame-Übertragungen durch den Prozess zur Bestätigung des Datenblockempfangs (Block Acknowledgement (ACK)) ausgeführt werden. Der gültige Bereich ist **0** bis **65535** ms. Der Standardwert ist **0**, was einer Deaktivierung der Zeitüberschreitung gleichkommt.

Aggregation Window Size (Größe des Aggregations-Fensters) Mit dieser Option wird die maximale Anzahl der ohne Empfang eines ACK übertragenen Pakete festgelegt. Der gültige Bereich ist **0** bis **64**. Der Standardwert ist **64**.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Best Effort (Beste Bemühung)

Use Aggregation (Aggregation verwenden) Diese Option definiert, ob die MAC-Ebene (Media Access Control) eine ADDBA-Sitzung (Add Block Acknowledgement) einrichtet oder nicht. Der Standardwert ist **Yes** (Ja). Wählen Sie **No** (Nein), um diese Option zu deaktivieren.

Accept Aggregation (Aggregation annehmen) Mit dieser Option wird festgelegt, ob die MAC-Ebene eine ADDBA-Anforderung annimmt oder nicht. Der Standardwert ist **Yes** (Ja). Wählen Sie **No** (Nein), um diese Option zu deaktivieren.

Max. Number of Packets in Aggregation (Max. Anzahl der Pakete in der Aggregation) Diese Option definiert die maximale Anzahl der Pakete (Sub-Frames) in einer Aggregation. Der gültige Bereich ist **0** bis **10**. Der Standardwert ist **10**.

Max. Aggregation Size (Max. Größe der Aggregation) Diese Option definiert die maximale Größe der Aggregation (in Byte). Der gültige Bereich ist **0** bis **20000**. Der Standardwert ist **16000**.

Timeout Interval (Zeitüberschreitungs-Intervall) Mit dieser Option wird das Zeitintervall festgelegt, vor dessen Ablauf die Aggregation mit einem „Abschlussstatus" geschlossen werden sollte, damit das Zeitlimit nicht überschritten wird. Der gültige Bereich ist **0** bis **100** ms. Der Standardwert ist **3**.

Size of Packet in Aggregation (Min. Größe der Pakete in der Aggregation) Diese Option definiert die minimale Größe (in Byte) der Pakete, die in der Aggregation zusammengestellt werden können. Der gültige Bereich ist **0** bis **1500**. Der Standardwert ist **10**.

ADDBA Timeout (ADDBA-Zeitüberschreitung) Mit dieser Option wird das Zeitintervall festgelegt, nach dessen Ablauf die ADDBA-Einrichtung abgebrochen wird, sofern innerhalb dieses Zeitraums keine Frame-Übertragungen durch den Prozess zur Bestätigung des Datenblockempfangs (Block Acknowledgement (ACK)) ausgeführt werden. Der gültige Bereich ist **0** bis **65535** ms. Der Standardwert ist **0**, was einer Deaktivierung der Zeitüberschreitung gleichkommt.

Aggregation Window Size (Größe des Aggregations-Fensters) Mit dieser Option wird die maximale Anzahl der ohne Empfang eines ACK übertragenen Pakete festgelegt. Der gültige Bereich ist **0** bis **64**. Der Standardwert ist **64**.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Video

Use Aggregation (Aggregation verwenden) Diese Option definiert, ob die MAC-Ebene (Media Access Control) eine ADDBA-Sitzung (Add Block Acknowledgement) einrichtet oder nicht. Der Standardwert ist **Yes** (Ja). Wählen Sie **No** (Nein), um diese Option zu deaktivieren.

Accept Aggregation (Aggregation annehmen) Mit dieser Option wird festgelegt, ob die MAC-Ebene eine ADDBA-Anforderung annimmt oder nicht. Der Standardwert ist **Yes** (Ja). Wählen Sie **No** (Nein), um diese Option zu deaktivieren.

Max. Number of Packets in Aggregation (Max. Anzahl der Pakete in der Aggregation) Diese Option definiert die maximale Anzahl der Pakete (Sub-Frames) in einer Aggregation. Der gültige Bereich ist **0** bis **7**. Der Standardwert ist **7**.

Max. Aggregation Size (Max. Größe der Aggregation) Diese Option definiert die maximale Größe der Aggregation (in Byte). Der gültige Bereich ist **0** bis **16000**. Der Standardwert ist **12000**.

Timeout Interval (Zeitüberschreitungs-Intervall) Mit dieser Option wird das Zeitintervall festgelegt, vor dessen Ablauf die Aggregation mit einem „Abschlussstatus" geschlossen werden sollte, damit das Zeitlimit nicht überschritten wird. Der gültige Bereich ist **0** bis **100** ms. Der Standardwert ist **3**.

Size of Packet in Aggregation (Min. Größe der Pakete in der Aggregation) Diese Option definiert die minimale Größe (in Byte) der Pakete, die in der Aggregation zusammengestellt werden können. Der gültige Bereich ist **0** bis **1500**. Der Standardwert ist **10**.

ADDBA Timeout (ADDBA-Zeitüberschreitung) Mit dieser Option wird das Zeitintervall festgelegt, nach dessen Ablauf die ADDBA-Einrichtung abgebrochen wird, sofern innerhalb dieses Zeitraums keine Frame-Übertragungen durch den Prozess zur Bestätigung des Datenblockempfangs (Block Acknowledgement (ACK)) ausgeführt werden. Der gültige Bereich ist **0** bis **65535** ms. Der Standardwert ist **0**, was einer Deaktivierung der Zeitüberschreitung gleichkommt.

Aggregation Window Size (Größe des Aggregations-Fensters) Mit dieser Option wird die maximale Anzahl der ohne Empfang eines ACK übertragenen Pakete festgelegt. Der gültige Bereich ist **0** bis **64**. Der Standardwert ist **64**.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Voice

Use Aggregation (Aggregation verwenden) Diese Option definiert, ob die MAC-Ebene (Media Access Control) eine ADDBA-Sitzung (Add Block Acknowledgement) einrichtet oder nicht. Der Standardwert ist **Yes** (Ja). Wählen Sie **No** (Nein), um diese Option zu deaktivieren.

Accept Aggregation (Aggregation annehmen) Mit dieser Option wird festgelegt, ob die MAC-Ebene eine ADDBA-Anforderung annimmt oder nicht. Der Standardwert ist **Yes** (Ja). Wählen Sie **No** (Nein), um diese Option zu deaktivieren.

Max. Number of Packets in Aggregation (Max. Anzahl der Pakete in der Aggregation) Diese Option definiert die maximale Anzahl der Pakete (Sub-Frames) in einer Aggregation. Der gültige Bereich ist **0** bis **2**. Der Standardwert ist **2**.

Max. Aggregation Size (Max. Größe der Aggregation) Diese Option definiert die maximale Größe der Aggregation (in Byte). Der gültige Bereich ist **0** bis **16000**. Der Standardwert ist **10000**.

Timeout Interval (Zeitüberschreitungs-Intervall) Mit dieser Option wird das Zeitintervall festgelegt, vor dessen Ablauf die Aggregation mit einem „Abschlussstatus" geschlossen werden sollte, damit das Zeitlimit nicht überschritten wird. Der gültige Bereich ist **0** bis **100** ms. Der Standardwert ist **10**.

Size of Packet in Aggregation (Min. Größe der Pakete in der Aggregation) Diese Option definiert die minimale Größe (in Byte) der Pakete, die in der Aggregation zusammengestellt werden können. Der gültige Bereich ist **0** bis **1500**. Der Standardwert ist **10**.

ADDBA Timeout (ADDBA-Zeitüberschreitung) Mit dieser Option wird das Zeitintervall festgelegt, nach dessen Ablauf die ADDBA-Einrichtung abgebrochen wird, sofern innerhalb dieses Zeitraums keine Frame-Übertragungen durch den Prozess zur Bestätigung des Datenblockempfangs (Block Acknowledgement (ACK)) ausgeführt werden. Der gültige Bereich ist **0** bis **65535** ms. Der Standardwert ist **0**, was einer Deaktivierung der Zeitüberschreitung gleichkommt.

Aggregation Window Size (Größe des Aggregations-Fensters) Mit dieser Option wird die maximale Anzahl der ohne Empfang eines ACK übertragenen Pakete festgelegt. Der gültige Bereich ist **0** bis **64**. Der Standardwert ist **64**.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Wireless > Advanced Wireless Settings (Erweiterte Wireless-Einstellungen)

Konfigurieren Sie die erweiterten Wireless-Einstellungen der Bridge. Diese Einstellungen sollten nur von einem erfahrenen Administrator angepasst werden, da falsche Einstellungen die Leistung des Routers im Wireless-Betrieb beeinträchtigen können.



HINWEIS
Die Einstellungen im Fenster *Advanced Wireless Settings* (Erweiterte Wireless-Einstellungen) sind auf fortgeschrittene Nutzer zugeschnitten.

Erweiterte Wireless-Einstellungen

Mit Low-Density Parity-Check Code (LDPC) wird die Fehlerkorrektur aktiviert bzw. deaktiviert, um die Wahrscheinlichkeit von Datenverlusten auf hochfrequentierten Kanälen zu senken. Der Algorithmus für die Datenratenanpassung deaktiviert automatisch die LDPC-Kodierung, wenn die PHY-Datenraten den Wert von 162 überschreiten. Behalten Sie zur Verwendung der erweiterten LDCP-Fehlerkorrektur die Standardeinstellung **Yes** (Ja) bei. Anderenfalls wählen Sie **No** (Nein).

ERP Protection Type (ERP-Schutztyp) Mit dieser Option legen Sie den Schutz von OFDM-Paketen bei 802.11b-Stationen im Wireless-Netzwerk fest. Durch das Senden von RTS/CTS- CTS2Self-Paketen in 802.11b-Raten informiert die Bridge das Wireless-Netzwerk darüber, dass OFDM-Pakete übertragen werden und schützt die Pakete innerhalb des Wireless-Netzwerks. Die RTS/CTS- und CTS2Self-Pakete kreieren einen Overhead, der zu einer geringeren Durchsatzrate führen kann.

Die RTS/CTS-Option sorgt für eine bessere Abdeckung, bietet aber im Vergleich zu CTS2Self geringere Durchsatzraten, da die RTS/CTS-Option eine Bestätigung durch das empfangende Gerät beinhaltet. Behalten Sie zur Nutzung der RTS/CTS-Option die Standardeinstellung **RTS/CTS** bei. Die Option **None** (Keine) kann zu Konflikten zwischen OFDM- und CCK-Paketen führen. Wählen Sie **None** (Keine), um diese Option zu nutzen. Wählen Sie **CTS2Self**, um die Option **CTS2Self** zu nutzen.

11n Protection Type (11n-Schutztyp) Mit dieser Option können Sie den Schutz von HT-Geräten (non-High Throughput) im Wireless-Netzwerk konfigurieren. Erkennt der Wireless-Router (oder Access Point) eine Verbindung zu einem vorhandenen HT-Gerät, sendet er vor jeder Datenübertragung ein Signal zur Nutzung von RTS/CTS- oder CTS2Self-Mechanismen an alle HT-Geräte. Diese Funktion unterstützt auch alle standardmäßigen 802.11n-Schutzmechanismen, einschließlich MIMO.

Die RTS/CTS-Option sorgt für eine bessere Abdeckung, bietet aber im Vergleich zu CTS2Self geringere Durchsatzraten, da die RTS/CTS-Option eine Bestätigung durch das empfangende Gerät beinhaltet. Behalten Sie zur Nutzung der RTS/CTS-Option die Standardeinstellung **RTS/CTS** bei. Die Option **None** (Keine) kann zu Konflikten zwischen HT- und vorhandenen Paketen führen. Wählen Sie **None** (Keine), um diese Option zu nutzen. Wählen Sie **CTS2Self**, um die Option **CTS2Self** zu nutzen.

Percentage of maximal transmit power (Prozentsatz der maximalen Übertragungsleistung) Mit dieser Option können Sie den Prozentsatz der maximalen Übertragungsleistung im Verhältnis zu regulatorischen Domänenbeschränkungen festlegen. Wenn die regulatorische Domänenbeschränkung beispielsweise Übertragungen von bis zu 20 dB zulässt, kann bei einer Einstellung auf 50 % maximal mit 10 dB übertragen werden. Wählen Sie den gewünschten Prozentsatz aus. **12 %**, **25 %**, **50 %** oder **100 %**. Die Standardeinstellung ist **100 %**.

QoS Classification Type (QoS-Klassifizierungstyp) Mit dieser Option können Sie für die 802.1D- oder 802.1Q-Zuordnung im Feld *IP DSCP/TOS* WMM-Prioritäten festlegen (Background (Hintergrund), Best Effects (Beste Effekte), Video, Voice (Sprache)). Behalten Sie die Standardeinstellung **802.1D** bei, oder wählen Sie die von einigen IPTV-Streams verwendete Einstellung **802.1Q**.

Re-establish Ethernet connection when initiating wireless connection (Ethernet-Verbindung bei Aufbau der Wireless-Verbindung) **wieder herstellen** Um die DHCP-Erkennung über das der Bridge nachgeordnete Gerät auszulösen, setzt die Bridge den Ethernet-Link zwischen der Bridge und dem Gerät jedesmal zurück, wenn eine Wireless-Verbindung hergestellt wird. Wählen Sie **No** (Nein), um diesen Vorgang zu deaktivieren. Ansonsten behalten Sie die Standardeinstellung **Yes** (Ja) bei.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Administration (Verwaltung) > Management (Verwaltungsfunktionen)

Verwenden Sie dieses Fenster, -um bestimmte Bridge-Funktionen zu verwalten: Zugriff auf das browserbasierte Dienstprogramm, Sichern der Konfigurationsdatei und Neustart.



Verwaltungsfunktionen

Bridge-Zugriff

Schützen Sie den Zugriff auf das browserbasierte Dienstprogramm mit einem Passwort.

Bridge Password (Bridge-Passwort) Geben Sie ein neues Passwort für die Bridge ein.

Re-enter to confirm (Zur Bestätigung erneut eingeben) Geben Sie das Passwort zur Bestätigung erneut ein.

Idle Timeout (Maximale Leerlaufzeit) Sie können eine Zeitspanne festlegen, nach der Sie automatisch abgemeldet werden. Der gültige Bereich ist **60** bis **3600** Sekunden. Der Standardwert ist **600**.

Web-Zugriff

Access via Wireless (Wireless-Zugriff) Wenn Sie die Bridge in einer öffentlichen Domäne verwenden, die für Ihre Gäste über Wireless-Zugriff verfügbar ist, können Sie den Wireless-Zugriff auf das webbasierte Dienstprogramm der Bridge deaktivieren. Sie können nur über eine kabelgebundene Verbindung auf das webbasierte Dienstprogramm zugreifen, wenn Sie die Einstellung deaktivieren. Klicken Sie auf **Enabled** (Aktiviert), um den Wireless-Zugriff auf das Dienstprogramm zu aktivieren, oder klicken Sie auf **Disabled** (Deaktiviert), um den Wireless-Zugriff auf das Dienstprogramm zu deaktivieren.

Sichern und Wiederherstellen

Backup (Sichern) Klicken Sie auf **Backup Configurations** (Konfigurationen sichern), um die Konfigurationsdatei der Bridge zu sichern. Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Restore (Wiederherstellen) Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie die Konfigurationsdatei. Klicken Sie auf **Restore Configurations** (Konfigurationen wiederherstellen).

Neustart des Systems

Reboot (Neustart) Klicken Sie auf **Start to Reboot** (Neustarten), um die Bridge neu zu starten.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Verwaltung > Werkseinstellungen

In diesem Fenster setzen Sie die Bridge-Konfiguration auf die Werkseinstellungen zurück.

Werkseinstellungen

Restore All Settings (Alle Einstellungen wiederherstellen) Klicken Sie auf **Restore All Settings** (Alle Einstellungen wiederherstellen), um die Bridge auf die Werkseinstellungen zurückzusetzen. Alle von Ihnen gespeicherten Einstellungen gehen verloren, wenn die Standardeinstellungen wiederhergestellt werden.



Verwaltung > Firmware aktualisieren

In diesem Fenster können Sie die Firmware der Bridge aktualisieren. Aktualisieren Sie die Firmware nur, wenn Probleme mit der Bridge auftreten oder die neue Firmware eine Funktion enthält, die Sie verwenden möchten.



Laden Sie vor Aktualisierung der Firmware die Aktualisierungsdatei für die Bridge-Firmware von der Linksys Website unter **www.Linksys.com/support** herunter.

Firmware aktualisieren

Please select a file to upgrade the firmware (Wählen Sie eine Datei für die Aktualisierung der Firmware aus): Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie die Firmware-Aktualisierungsdatei aus. Klicken Sie dann auf **Start to Upgrade** (Aktualisierung starten), und folgen Sie den Anweisungen auf dem Bildschirm.

Status > Bridge

Hier werden die aktuellen Statusinformationen der Bridge angezeigt.



Bridge-Informationen

Firmware Version (Firmware-Version) Hier wird die aktuelle Firmware der Bridge angezeigt.

Lokales Netzwerk

Local MAC Address (Lokale MAC-Adresse) Hier wird die MAC-Adresse der Bridge im lokalen Ethernet-Netzwerk angezeigt.

IP Address (IP-Adresse) Die IP-Adresse der Bridge, wie sie in Ihrem Netzwerk angezeigt wird.

Subnet Mask (Subnetzmaske) Hier wird die für das lokale Netzwerk konfigurierte Subnetzmaske angezeigt.

Status > Wireless

Hier werden Informationen zu Ihrem Wireless-Netzwerk angezeigt.



Wireless-Geräte

Link Status (Verbindungsstatus) Hier wird der Verbindungsstatus zum Wireless-Netzwerk angezeigt.

MAC Address (MAC-Adresse) Hier wird die MAC-Adresse der Bridge im lokalen Wireless-Netzwerk angezeigt.

Netzwerkname (SSID) Hier wird der Name des Wireless-Netzwerks oder die SSID angezeigt.

BSSID Hier wird die Wireless-MAC-Adresse des angeschlossenen Wireless-Routers (oder Access Points) angezeigt.

Radio Band (Frequenzband) Das Frequenzband des angezeigten Wireless-Netzwerks.

Channel Width (Funkkanalbreite) Hier wird die von Ihrem Wireless-Netzwerk verwendete Funkkanalbreite in MHz angezeigt.

Wide Channel (Zusatzkanal) Abhängig von den Kanaleinstellungen Ihres Netzwerkrouters wird hier der Zusatzkanal angezeigt. Wenn Sie **40-MHz-Zusatzkanal** als Einstellung für Frequenzband oder Funkkanalbreite ausgewählt haben, ist dies der primäre Kanal für Wireless-N.

Standard Channel (Standardkanal) Hier werden die Einstellungen des Standardkanals angezeigt. Wenn Sie **40-MHz-Zusatzkanal** als Einstellung für Frequenzband oder Funkkanalbreite ausgewählt haben, ist der Standardkanal ein sekundärer Kanal für Wireless-N.

Bit Rate (Bitrate) Hier wird die Datenübertragungsrate angezeigt.

Signal Hier wird der Prozentsatz der Signalstärke angezeigt. 100 % ist die höchstmögliche, 0 % die geringstmögliche Signalstärke.

Security (Sicherheit) Hier wird die Sicherheitsmethode Ihres Wireless-Netzwerks angezeigt.

Fehlerbehebung

WES610N/WET610N

Ihr Computer oder ein anderes kabelgebundenes Ethernet-Gerät kann nicht mit dem Wireless-Router kommunizieren.

1. Öffnen Sie das browserbasierte Dienstprogramm der Bridge.
2. Stellen Sie sicher, dass der Eintrag unter Network Name (SSID) (Netzwerkname, SSID) im Fenster *Basic Wireless Settings* (Grundlegende Wireless-Einstellungen) mit dem Namen Ihres Wireless-Netzwerks übereinstimmt.
3. Stellen Sie sicher, dass die Sicherheitseinstellungen (WPA, WPA2 oder WEP) mit den Sicherheitseinstellungen Ihres Wireless-Netzwerks übereinstimmen.

Die IP-Adresse Ihres Netzwerks muss geändert werden.

Wenn die Bridge mit einem Netzwerk mit DHCP-Server verbunden ist (in der Regel der Netzwerk-Router), ruft die Bridge die IP-Adresse vom DHCP-Server ab. Wenn kein DHCP-Server erkannt wird, wird für die Bridge die statische Standard-IP-Adresse **169.254.1.250** verwendet.

Wenn Sie möchten, dass die Bridge immer die statische IP-Adresse verwendet, gehen Sie wie folgt vor:

1. Öffnen Sie das browserbasierte Dienstprogramm der Bridge.
2. Klicken Sie auf die Registerkarte **Network Setup** (Netzwerk-Einrichtung).
3. Wählen Sie im Dropdown-Menü *Network Connection Type* (Netzwerkverbindungstyp) die Option **Static IP** (Statische IP-Adresse) aus.
4. Füllen Sie die Felder *Static IP Address* (Statische IP-Adresse), *Subnet Mask* (Subnetzmaske) und *Default Gateway* (Standard-Gateway) aus.
5. Klicken Sie auf **Save Settings** (Einstellungen speichern).

Der Computer mit Bridge-Unterstützung oder ein anderes kabelgebundenes Ethernet-Gerät kommunizieren nicht mit einem anderen Gerät mit Wireless-Unterstützung (wie einem Computer oder Drucker).

Überprüfen Sie Folgendes:

- Stellen Sie sicher, dass das Gerät mit Wireless-Unterstützung sich im gleichen Wireless-Netzwerk befindet wie der Computer oder ein anderes kabelgebundenes Ethernet-Gerät, das mit der Bridge verbunden ist.
- Stellen Sie sicher, das der Netzwerkname (SSID) für alle Geräte im kabellosen Netzwerk verwendet wird.
- Stellen Sie sicher, dass alle Geräte sich im gleichen IP-Netzwerk befinden und kompatible IP-Adressen verwenden.

Das browserbasierte Dienstprogramm akzeptiert das Passwort nicht.

Überprüfen Sie Folgendes:

- Beim Passwort wird zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie daher sicher, dass Sie die korrekte Groß- und Kleinschreibung verwenden, wenn Sie das Passwort eingeben.
- Wenn Sie das Passwort vergessen haben, können Sie die Bridge auf die Werkseinstellung zurücksetzen.

 Halten Sie die Taste **Reset** (Zurücksetzen) für circa fünf Sekunden gedrückt; das Passwort wird auf den Werksstandard **admin** zurückgesetzt. Alle anderen Bridge-Einstellungen werden ebenfalls auf Werkseinstellung zurückgesetzt. (Geben Sie im Feld **Password** (Passwort) *admin* ein, um auf das browserbasierte Dienstprogramm zuzugreifen.)

Wenn Sie Änderungen über das browserbasierte Dienstprogramm vornehmen, werden die neuen Einstellungen nicht auf dem Bildschirm angezeigt.

Klicken Sie im Webbrowser auf **Refresh** (Aktualisieren). Wenn die neuen Einstellungen nicht angezeigt werden, folgen Sie der nachstehenden Anleitung:

1. Trennen Sie das Netzteil von der Bridge.
2. Warten Sie 5 Sekunden, und schließen Sie das Netzteil wieder an der Bridge an.
3. Klicken Sie im Webbrowser auf **Refresh** (Aktualisieren).

WEB
Wenn Ihre Fragen hier nicht beantwortet wurden, finden Sie weitere Informationen auf der Linksys Website unter **Linksys.com/support**

Spezifikationen

WES610N

Modell	WES610N
Standards	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LEDs	Power, Ethernet, Wi-Fi Protected Setup™, Wireless, individueller Ethernet-Link und Aktivität
Ports	Ethernet (4), Power
Tasten	Reset, Wi-Fi Protected Setup
Kabeltyp	CAT5e
Antennen	3 (intern)
Antennenverbindungstyp	k. A.
Abnehmbar (Ja/Nein)	Nein
Modulationen	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	802.11a: 15 dBm (typisch) bei 54 Mbit/s 802.11b: 19 dBm (typisch) bei 11 Mbit/s 802.11g: 16 dBm (typisch) bei 54 Mbit/s 802.11n (2,4 GHz): 18 dBm (typisch) bei MCS15 802.11n (5 GHz): 16 dBm (typisch) bei MCS15
Empfangsempfindlichkeit	802.11a: -72 dBm (typisch) bei 54 Mbit/s 802.11b: -85 dBm (typisch) bei 11 Mbit/s 802.11g: -73 dBm (typisch) bei 54 Mbit/s 802.11n (20 MHz): -75 dBm (typisch) bei MCS15 802.11n (40 MHz): -69 dBm (typisch) bei MCS15
Antennengewinn in dBi	1
Wireless-Sicherheit	WEP Wi-Fi Protected Access™ (WPS), Wi-Fi Protected Access™ 2 (WPA2)
Sicherheitsschlüssel/Bit	Verschlüsselung mit bis zu 128 Bit

Betriebsbedingungen

Abmessungen	177 x 128 x 68 mm
Gewicht	295 g
Zertifizierung	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/Draft-N), WPA2™, Wi-Fi Protected Setup, WMM®
Netzstrom	12 V, 1 A
Betriebstemperatur	0 bis 40 °C
Lagerungstemperatur	-20 bis 60 °C
Luftfeuchtigkeit bei Betrieb	10 bis 85 % (nicht kondensierend)
Luftfeuchtigkeit bei Lagerung	5 bis 90 % (nicht kondensierend)

Technische Änderungen vorbehalten.

WET610N

Modell	WET610N
Standards	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LEDs	Power, Ethernet, Wi-Fi Protected Setup™, Wireless
Ports	Ethernet, Power
Tasten	Reset, Wi-Fi Protected Setup
Kabeltyp	CAT5e
Antennen	3 (intern)
Antennenverbindungstyp	k. A.
Abnehmbar (Ja/Nein)	Nein
Modulationen	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	802.11a: 15 dBm (typisch) bei 54 Mbit/s 802.11b: 18 dBm (typisch) bei 11 Mbit/s 802.11g: 16 dBm (typisch) bei 54 Mbit/s 802.11n: 12 dBm (typisch) bei 130 Mbit/s (HT20), 270 Mbit/s (HT40)
Empfangsempfindlichkeit	802.11a: -72 dBm (typisch) bei 54 Mbit/s 802.11b: -85 dBm (typisch) bei 11 Mbit/s 802.11g: -73 dBm (typisch) bei 54 Mbit/s 802.11n: -70 dBm (typisch) bei MCS15/2,4 GHz, -69 dBm (typisch) bei MCS15/5,0 GHz
Antennengewinn in dBi	1
Wireless-Sicherheit	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Sicherheitsschlüssel/Bit	Verschlüsselung mit bis zu 128 Bit

Betriebsbedingungen

Maße	145 x 106 x 52 mm
Gewicht	159 g
Zertifizierung	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/Draft-N), WPA2™, Wi-Fi Protected Setup, WMM®
Netzstrom	12 V, 1 A
Betriebstemperatur	0 bis 40 °C
Lagerungstemperatur	-20 bis 60 °C
Luftfeuchtigkeit bei Betrieb	10 bis 85 % (nicht kondensierend)
Luftfeuchtigkeit bei Lagerung	5 bis 90 % (nicht kondensierend)

Technische Änderungen vorbehalten.

Linksys.com/support

Cisco, das Cisco Logo und Linksys sind Marken bzw. eingetragene Marken von Cisco und/oder dessen Zweigunternehmen in den USA und anderen Ländern.
Eine Liste der eingetragenen Marken von Cisco finden Sie unter www.cisco.com/go/trademarks. Alle anderen in diesem Dokument genannten Marken sind Eigentum ihrer jeweiligen Rechtsinhaber.

© 2011 Cisco und/oder deren Zweigunternehmen. Alle Rechte vorbehalten.

3425-01249



Brugervejledning

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Indholdsfortegnelse

Produktoversigt

LED-panel 2
Portpanel 3

Tjekliste for trådløs sikkerhed

Skift det trådløse netværks standardnavn eller SSID 4
Skift standardadgangskoden 4
Slå MAC-adressefiltrering til 4
Slå kryptering til 4

Generelle retningslinjer for netværkssikkerhed 4
Yderligere sikkerhedstip 5

Avanceret konfiguration

Sådan får du adgang til det browserbaserede hjælpeprogram . . . 6

Setup (Konfiguration) > Basic Setup (Grundlæggende konfiguration) 7
Language (Sprog) 7
Network Setup (Netværkskonfiguration) 7

Wireless (Trådløs) > Basic Wireless Settings (Grundlæggende trådløse indstillinger) 7
Basic Wireless Settings (Grundlæggende trådløse indstillinger) 8
Wireless Security (Trådløs sikkerhed) 8
Wi-Fi Protected Setup 9

Wireless (Trådløs) > Wireless Network Site Survey (Undersøgelse af trådløst netværkswebsted) 10
Wireless Network Site Survey (Undersøgelse af trådløst netværkswebsted) 10

Wireless (Trådløs) > WMM® 11
WMM 12

Wireless (Trådløs) > Advanced Wireless Settings (Avancerede trådløse indstillinger) 13
Advanced Wireless (Avanceret trådløs) 13

Administration > Management (Styring) 14
Management (Styring) 14

Administration > Factory Defaults (Standardindstillinger fra fabrikken) 15
Factory Defaults (Standardindstillinger fra fabrikken) 15

Administration > Upgrade Firmware (Opgrader firmware) . . . 15
Upgrade Firmware (Opgrader firmware) 15

Status > Bridge (Bro) 15
Bridge Information (Oplysninger om bro) 16
Local Network (Lokalt netværk) 16

Status > Wireless (Trådløs) 16
Wireless (Trådløs) 16

Fejlfinding

WES610N/WET610N 17

Specifikationer

WES610N 18
WET610N 19

Produktoversigt

Tak, fordi du har valgt at købe en Linksys Dual-Band N Entertainment Bridge. Broen kan bruges til tilslutning af en vilkårlig kabelforbundet Ethernet-enhed til et trådløst netværk. Broen anvender Dual-Band Trådløs-N og er derfor kompatibel med alle Trådløs-N-, -G-, -A- eller -B-routere eller adgangspunkter. Følg trinnene i mappen CD i forbindelse med den første installation. Konfigurer avancerede indstillinger ved hjælp af det relevante browserbaserede hjælpeprogram.

LED-panel



WES610N WET610N

Trådløs (blå) Den trådløse indikator lyser, når der er oprettet trådløs forbindelse. Indikatoren blinker, når broen aktivt sender eller modtager data over det trådløse netværk.

Knappen Wi-Fi Protected Setup Hvis netværksrouteren understøtter Wi-Fi Protected Setup og bruger WPA- eller WPA2-sikkerhed, kan du oprette automatisk forbindelse til broen ved hjælp af Wi-Fi Protected Setup. Du kan finde flere oplysninger om, hvordan du bruger Wi-Fi Protected Setup, under "Wireless (Trådløs) > Basic Wireless Settings (Grundlæggende trådløse indstillinger)" på side 7.

Wi-Fi Protected Setup-indikator (blå/gul) Indikatoren blinker blåt i to minutter i forbindelse med Wi-Fi Protected Setup. Den lyser blåt, når trådløs sikkerhed er aktiveret. Hvis der opstår fejl under Wi-Fi Protected Setup-processen, lyser indikatoren gult. Kontroller, at netværksrouteren understøtter Wi-Fi Protected Setup. Vent, indtil indikatoren holder op med at lyse, og prøv igen.

Ethernet (blå) Ethernet-indikatoren lyser, når der bruges en kabelforbindelse. Indikatoren blinker, når broen aktivt sender eller modtager data over Ethernet-porten(e).

Strøm (blå) Strømindikatoren lyser, når der er sluttet strøm til broen.

Portpanel



WES610N WET610N

Ethernet Ethernet-porten(e) bruges til at forbinde broen med en computer eller anden Ethernet-netværksenhed. WES610N har fire porte, og WET610N har en enkelt port.

Nulstilling Du kan nulstille broen til standardindstillingerne fra fabrikken på to måder: Du kan enten trykke på nulstillingsknappen og holde den inde i ca. fem sekunder, eller du kan gendanne standardindstillingerne under Administration > Factory Defaults (Standardindstillinger fra fabrikken) i broens browserbaserede hjælpeprogram. WES610N har en nulstillingsknap under bunden af enheden, og WET610N har en nulstillingsknap på portpanelet på bagsiden af enheden.

Strøm Strømporten bruges til at slutte broen til den medfølgende strømadapter.

Tjekliste for trådløs sikkerhed

Trådløse netværk er både praktiske og nemme at installere og bliver mere og mere almindelige i private hjem, hvor der er adgang til højhastighedsinternet. Et trådløst netværk fungerer ved at sende oplysninger via radiobølger og kan derfor være mere sårbart over for uautoriseret adgang end et traditionelt kabelnetværk. Det er også muligt at opfange signaler fra det trådløse netværk på samme måde som signaler fra mobiltelefoner eller trådløse telefoner. Da du ikke fysisk kan forhindre andre i at oprette forbindelse til dit trådløse netværk, er det vigtigt, at du træffer andre foranstaltninger for at beskytte sikkerheden på netværket.

Skift det trådløse netværks standardnavn eller SSID

Trådløse enheder har et trådløst netværksnavn eller SSID (Service Set Identifier), som konfigureres fra fabrikken. Dette er det trådløse netværks standardnavn, som kan indeholde op til 32 tegn. Trådløse produkter fra Linksys bruger **linksys** som navn på det trådløse netværk som standard. Det anbefales, at du ændrer det trådløse netværks navn til et entydigt navn, så du kan skelne dit trådløse netværk fra andre trådløse netværk i nærheden, men undlad at bruge personlige oplysninger i navnet (f.eks. dit cpr-nummer), da oplysningerne kan ses af alle, som søger efter trådløse netværk.

Skift standardadgangskoden

I forbindelse med trådløse produkter, f.eks. adgangspunkter og routere, bliver du bedt om at angive en adgangskode, når du vil ændre de tilhørende indstillinger. Disse enheder har muligvis en standardadgangskode, som er angivet fra fabrikken. Linksys-standardadgangskoden er **admin**. Hackere kender disse standarder og forsøger muligvis at bruge dem til at få adgang til din trådløse enhed og ændre dine netværksindstillinger. Hvis du vil forebygge uautoriserede ændringer, skal du tilpasse enhedens adgangskode, så den er svær at gætte.

Slå MAC-adressefiltrering til

Linksys-routere giver dig mulighed for at slå MAC-adressefiltrering (Media Access Control) til. MAC-adressen er en entydig serie af tal og bogstaver, som knyttes til den enkelte netværksenhed. Når MAC-adressefiltrering er slået til, begrænses adgangen til det trådløse netværk til trådløse enheder med bestemte MAC-adresser. Du kan f.eks. angive MAC-adressen for alle computere i dit hjem, så det kun er disse computere, der kan få adgang til det trådløse netværk.

Slå kryptering til

Kryptering beskytter data, som overføres over et trådløst netværk. WPA/WPA2 (Wi-Fi Protected Access) og WEP (Wired Equivalent Privacy) tilbyder forskellige niveauer af sikkerhed til trådløs kommunikation.

Et netværk, som er krypteret med WPA/WPA2, er bedre beskyttet end et netværk, som er krypteret med WEP, fordi WPA/WPA2 anvender dynamisk nøglekryptering. Det anbefales, at du anvender det højeste krypteringsniveau, som netværksudstyret understøtter, for at beskytte data, der sendes over netværket, optimalt.

WEP er en ældre krypteringsstandard og er muligvis den eneste tilgængelige indstilling på visse ældre enheder, som ikke understøtter WPA.

Generelle retningslinjer for netværkssikkerhed

Trådløs netværkssikkerhed er ikke meget bevendt, hvis det underliggende netværk ikke er sikkert.

- Beskyt alle computere på netværket med adgangskoder, og beskyt individuelle filer, som indeholder følsomme data, med adgangskoder.
- Skift adgangskoder med jævne mellemrum.
- Installer antivirussoftware og personlig firewallsoftware.
- Slå fildeling fra (peer-to-peer). Nogle programmer åbner muligvis fildeling uden dit samtykke og/eller uden din viden.

Yderligere sikkerhedstip

- Anbring trådløse routere, adgangspunkter og gateways i sikker afstand til udvendige vægge og vinduer.
- Sluk for trådløse routere, adgangspunkter og gateways, når de ikke er i brug (om natten og i forbindelse med ferieperioder).
- Brug stærke adgangsord med mindst otte tegn. Brug en kombination af bogstaver og tal, og undlad at bruge ord, som findes i ordbogen.

Avanceret konfiguration

Broen er klar til brug, når du har konfigureret den ved at følge trinnene i mappen CD. Hvis du vil ændre de avancerede indstillinger for broen, skal du dog bruge broens browserbaserede hjælpeprogram. I dette kapitel beskrives de enkelte sider i hjælpeprogrammet samt de vigtigste funktioner på hver side. Du kan få adgang til hjælpeprogrammet fra webbrowseren på en computer, som har forbindelse til broen.

Det browserbaserede hjælpeprogram indeholder følgende overordnede faner: Setup (Konfiguration), Wireless (Trådløs), Administration og Status. Der vises yderligere faner, når du klikker på en af de overordnede faner.

Sådan får du adgang til det browserbaserede hjælpeprogram

Åbn det browserbaserede hjælpeprogram fra en webbrowser.

Hvis broen har forbindelse til et netværk med en DHCP-server (sædvanligvis netværksrouteren), får broen sin IP-adresse fra DHCP-serveren. Hvis der ikke er nogen DHCP-server, bruger broen den statiske IP-adresse **169.254.1.250** som standard. Hvis du har angivet en permanent statisk IP-adresse for broen via det browserbaserede hjælpeprogram, skal du i stedet angive den statiske IP-adresse.

BEMÆRK!
Hvis du ikke kender broens IP-adresse, kan du finde IP-adressen i routerens tabel over DHCP-klienter. Se dokumentationen til routeren.

Hvis du ikke kan finde broens IP-adresse, kan du nulstille broen ved at trykke på knappen **Reset** (Nulstil) på broen med en papirclips, som du har rettet ud, og holde den inde i cirka fem sekunder. Dermed nulstilles broen til standardindstillingerne fra fabrikken. Broen anmoder om en IP-adresse fra DHCP-serveren (sædvanligvis netværksrouteren). Hvis der ikke findes nogen DHCP-server, bruger broen den statiske IP-adresse **169.254.1.250** som standard, indtil den registrerer en DHCP-server og tildeles en dynamisk IP-adresse.

Hvis broen ikke er knyttet til en router og bruger standardindstillingerne fra fabrikken, skal du slutte en computer til broen via Ethernet for at få adgang til det webbaserede-hjælpeprogram. Du skal konfigurere Ethernet-forbindelsen på computeren med en statisk IP-adresse og en undernetmaske.

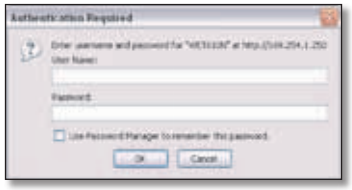
IP-adressen for Ethernet-adapteren skal angives til en bestemt IP-adresse.

1. Skriv **169.254.x.y** i feltet *IP address* (IP-adresse) (x skal erstattes af et tal mellem 1 og 254, og y skal erstattes af et tal mellem 0 og 255).
2. Skriv **255.255.0.0** i feltet *Subnet mask* (Undernetmaske).

BEMÆRK!
Fremgangsmåden til tildeling af en statisk IP-adresse til Ethernet-adapteren på computeren varierer afhængigt af operativsystemet. Du kan finde flere oplysninger i hjælpedokumentationen til det operativsystem, du bruger.

Når du har tildelt Ethernet-adapteren en statisk IP-adresse, skal du starte webbrowseren og angive adapterens IP-adresse (standardindstillingen er **169.254.1.250**) i feltet *Address* (Adresse). Tryk på **Enter**.

Der vises et skærmbillede, hvor du bliver bedt om at angive en adgangskode. Brugere, som ikke kører Windows XP, får vist et tilsvarende skærmbillede. Lad feltet *User name* (Brugernavn) være tomt. Angiv den adgangskode, du har oprettet i forbindelse med konfigurationen. Hvis du ikke har oprettet nogen adgangskode, skal du bruge standardadgangskoden **admin**. Du kan angive en ny adgangskode på skærmbilledet *Administration* > *Management* (Styring). Klik på **OK** for at fortsætte.



BEMÆRK!
Hvis skærmbilledet, hvor du bliver anmodet om at angive adgangskoden, ikke vises, skal du vente to minutter og derefter prøve igen.

Setup (Konfiguration) > Basic Setup (Grundlæggende konfiguration)

Det første skærmbillede, der vises, er skærmbilledet *Basic Setup* (Grundlæggende konfiguration). På dette skærmbillede kan du ændre sprog for det webbaserede hjælpeprogram eller netværksindstillingerne for den kabelforbundne Ethernet-forbindelse.





Language (Sprog)

Language (Sprog) bruges til at angive sprog for det browserbaserede hjælpeprogram. Vælg det ønskede sprog i rullemenuen.

Network Setup (Netværkskonfiguration)

Dette afsnit bruges til at angive, om broens IP-adresse hentes automatisk fra en DHCP-server, f.eks. netværksrouteren (Automatic Configuration - DHCP (Automatisk konfiguration – DHCP)), eller angives manuelt (Static IP (Statisk IP)).

Bridge IP (Broens IP) Hvis netværket har en DHCP-server, f.eks. netværksrouteren, som tildeler IP-adresser til netværksenhederne, skal du beholde standardindstillingen **Automatic Configuration - DHCP** (Automatisk konfiguration – DHCP). Broen anmoder om en IP-adresse fra DHCP-serveren (sædvanligvis netværksrouteren). Hvis der ikke findes nogen DHCP-server, bruger broen den statiske IP-adresse **169.254.1.250** som standard, indtil den registrerer en DHCP-server og tildeles en dynamisk IP-adresse.

Hvis du vil angive en permanent statisk IP-adresse for broen, skal du vælge **Static IP** (Statisk IP).

Hvis du vælger Static IP (Statisk IP), skal du udfylde følgende felter:

- **Static IP Address** (Statisk IP-adresse) Angiv en entydig IP-adresse, som skal bruges til at få adgang til det browserbaserede hjælpeprogram.
- **Subnet Mask** (Undernetmaske) Angiv undernetmasken for det kabelforbundne netværk.
- **Default Gateway** (Standard-gateway) Angiv IP-adressen for netværkets standard-gateway (i de fleste tilfælde er dette din router).

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Wireless (Trådløs) > Basic Wireless Settings (Grundlæggende trådløse indstillinger)

På skærmbilledet *Basic Wireless Settings* (Grundlæggende trådløse indstillinger) kan du konfigurere de grundlæggende trådløse indstillinger og sikkerhedsindstillinger for broen.

Broens indstillinger kan konfigureres enten manuelt eller via WPS (Wi-Fi Protected Setup). Wi-Fi Protected Setup er en funktion, som gør det nemt at konfigurere det trådløse netværk. Hvis netværksrouteren understøtter Wi-Fi Protected Setup og bruger WPA- eller WPA2-sikkerhed, kan du konfigurere broen automatisk ved hjælp af Wi-Fi Protected Setup.

Configuration View (Konfigurationsvisning) Vælg **Manual** (Manuel) for at konfigurere det trådløse netværk manuelt. Se **Basic Wireless Settings** (Grundlæggende trådløse indstillinger), **side 8**. Hvis du vil bruge Wi-Fi Protected Setup, skal du vælge **Wi-Fi Protected Setup**. Se **Wi-Fi Protected Setup**, **side 9**.

Basic Wireless Settings (Grundlæggende trådløse indstillinger)



Network Name (SSID) (Netværksnavn (SSID)) SSID'et er netværksnavnet, som deles med alle punkter på et trådløst netværk. SSID'et skal være identisk for alle enheder på det trådløse netværk. Der skelnes mellem store og små bogstaver i SSID'et, og det må ikke indeholder mere end 32 tegn (det er tilladt at bruge alle tegn på tastaturet). Kontroller, at indstillingen stemmer overens med indstillingen for den trådløse router eller adgangspunktet. Hvis du vil forbedre sikkerheden, skal du ændre standard-SSID'et (**linksys**) til et entydigt navn.

Wireless Security (Trådløs sikkerhed)

Broen understøtter følgende trådløse sikkerhedsindstillinger: WPA Personal, WPA2 Personal og WEP. WPA (Wi-Fi Protected Access) og WPA2 er stærkere sikkerhedsmetoder end WEP (Wired Equivalent Privacy). Du kan finde flere oplysninger om trådløs sikkerhed under "Tjekliste for trådløs sikkerhed", side 4.

Security Mode (Sikkerhedstilstand)

Vælg sikkerhedstilstanden for det trådløse netværk. Hvis du ikke ønsker at bruge trådløs sikkerhed, skal du bevare standardindstillingen **Disabled** (Deaktiveret).

BEMÆRK!
Husk, at alle enheder på det trådløse netværk SKAL bruge den samme sikkerhedsmetode og det samme adgangsord/den samme nøgle. Ellers kan de trådløse enheder ikke kommunikere med hinanden.

WPA Personal

WPA er en sikkerhedsstandard, som er stærkere end WEP-kryptering.



Encryption (Kryptering) WPA understøtter TKIP-krypteringsmetoden med dynamiske krypteringsnøgler.

Passphrase (Adgangsord) Angiv den nøgle, som deles af broen og den trådløse router eller adgangspunktet. Adgangsordet skal indeholde 8-63 tegn.

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

WPA2 Personal

WPA2 er en mere avanceret og mere sikker version af WPA.



Encryption (Kryptering) WPA2 understøtter krypteringsmetoderne TKIP og AES med dynamiske krypteringsnøgler. Vælg krypteringsmetoden **AES** eller **TKIP or AES** (TKIP eller AES). Standardindstillingen er **AES**.

Passphrase (Adgangsord) Angiv den nøgle, som deles af broen og den trådløse router eller adgangspunktet. Adgangsordet skal indeholde 8-63 tegn.

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

WEP

WEP er en grundlæggende krypteringsmetode, som er mindre sikker end WPA og WPA2.



Encryption (Kryptering) Vælg et WEP-krypteringsniveau, **40/64 bits (10 hex digits)** (40/64-bit (10 hexadecimale tal)) eller **104/128 bits (26 hex digits)** (104/128-bit (26 hexadecimale tal)). Standardindstillingen er **40/64 bits (10 hex digits)** (40/64-bit (10 hexadecimale tal)).

Key 1 (Nøgle 1) Angiv WEP-nøglen for netværket.

Tx Key (TX-nøgle) **Key 1** (Nøgle 1) er den overførselsnøgle, som anvendes af broen.

Authentication (Godkendelse) Standardindstillingen er **Auto**, som gør det muligt at bruge åben systemgodkendelse eller godkendelse med delt nøgle. Vælg **Open** (Åben) for at bruge åben systemgodkendelse, hvor afsenderen og modtageren ikke bruger en WEP-nøgle til godkendelse. Vælg **Shared** (Delt) for at bruge godkendelse med delt nøgle, hvor afsenderen og modtageren bruger en WEP-nøgle til godkendelse.

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Wi-Fi Protected Setup

Der er to tilgængelige metoder. Brug den metode, som er relevant for den router, du bruger.





Method #1 (Metode 1)

Brug denne metode, hvis din router har en knap til Wi-Fi Protected Setup.

1. Klik eller tryk på knappen **Wi-Fi Protected Setup** på routeren.
2. Klik på knappen **Wi-Fi Protected Setup** på skærmbilledet *Wi-Fi Protected Setup* for broen inden for to minutter.
3. Klik på **Close** (Luk), når broen er blevet konfigureret.

Skærmbilledet *Wi-Fi Protected Setup* viser Link Status (Linkstatus), Network Name (SSID) (Netværksnavn (SSID)) og Security method (Sikkerhedsmetode).

Method #2 (Metode 2)

Brug denne metode, hvis routeren anmoder om broens PIN-nummer.

1. Angiv PIN-nummeret på skærmbilledet *Wi-Fi Protected Setup* for **broen** på skærmbilledet *Wi-Fi Protected Setup* på **routeren**. Klik derefter på **Register** (Registrer) eller på den relevante knap. Nummeret er også angivet på etiketten under bunden af broen.
2. Klik på **OK** på skærmbilledet *Wi-Fi Protected Setup* på **broen**.
3. Klik på **Close** (Luk), når broen er blevet konfigureret.

Skærmbilledet *Wi-Fi Protected Setup* viser Link Status (Linkstatus), Network Name (SSID) (Netværksnavn (SSID)) og Security method (Sikkerhedsmetode).

Wireless (Trådløs) > Wireless Network Site Survey (Undersøgelse af trådløst netværkswebsted)

Klik på fanen **Wireless Network Site Survey** (Undersøgelse af trådløst netværkswebsted) for at starte en webstedsundersøgelse. På skærmbilledet *Wireless Network Site Survey* (Undersøgelse af trådløst netværkswebsted) vises de trådløse netværk, som broen har registreret.



Wireless Network Site Survey (Undersøgelse af trådløst netværkswebsted)

Number of Wireless Networks (Antal trådløse netværk) Det antal trådløse netværk, som broen har registreret, vises.

Select (Vælg) Klik på **Select** (Vælg) for at oprette forbindelse til et trådløst netværk. Klik derefter på **Connect** (Opret forbindelse).

Wireless Network Name (Trådløst netværksnavn) Det trådløse netværks netværksnavn eller SSID vises.

GHz Det trådløse netværks radiobånd vises.

Signal Signalstyrken i procent vises. 100 % er den kraftigste signalstyrke, og 0 % er den svageste.

Security (Sikkerhed) Hvis netværket understøtter Wi-Fi Protected Setup, vises ikonet Wi-Fi Protected Setup . Den sikkerhedsmetode, der anvendes af det trådløse netværk, vises.

Klik på **Refresh** (Opdater) for at opdatere oplysningerne på skærmen.

Når du har valgt et netværk, skal du klikke på **Connect** (Opret forbindelse). Der åbnes et nyt skærmbillede. Følg anvisningerne for den sikkerhedsmetode, som netværket anvender.

WPA



Network Name (SSID) (Netværksnavn (SSID)) Navnet på det valgte netværk vises automatisk.

Security Mode (Sikkerhedstilstand) WPA Personal vises automatisk.

Encryption (Kryptering) WPA understøtter TKIP-krypteringsmetoden med dynamiske krypteringsnøgler.

Passphrase (Adgangsord) Angiv den nøgle, som deles af broen og den trådløse router eller adgangspunktet. Adgangsordet skal indeholde 8-63 tegn.

Klik på **Refresh** (Opdater) for at opdatere oplysningerne på skærmen.

Når du har angivet sikkerhedsindstillingerne, skal du klikke på **Connect** (Opret forbindelse).

WPA2



Network Name (SSID) (Netværksnavn (SSID)) Navnet på det valgte netværk vises automatisk.

Security Mode (Sikkerhedstilstand) WPA2 Personal vises automatisk.

Encryption (Kryptering) WPA2 understøtter krypteringsmetoderne TKIP og AES med dynamiske krypteringsnøgler. Vælg krypteringsmetoden **AES** eller **TKIP or AES** (TKIP eller AES).

Passphrase (Adgangsord) Angiv den nøgle, som deles af broen og den trådløse router eller adgangspunktet. Adgangsordet skal indeholde 8-63 tegn.

Klik på **Refresh** (Opdater) for at opdatere oplysningerne på skærmen.

Når du har angivet sikkerhedsindstillingerne, skal du klikke på **Connect** (Opret forbindelse).

WEP



Network Name (SSID) (Netværksnavn (SSID)) Navnet på det valgte netværk vises automatisk.

Security Mode (Sikkerhedstilstand) WEP vises automatisk.

Encryption (Kryptering) Vælg et WEP-krypteringsniveau **40/64 bits (10 hex digits)** (40/64-bit (10 hexadecimale tal)) eller **104/128 bits (26 hex digits)** (104/128-bit (26 hexadecimale tal)).

Key 1 (Nøgle 1) Angiv WEP-nøglen for netværket.

Tx Key (TX-nøgle) **Key 1** (Nøgle 1) er den overførselsnøgle, som anvendes af broen.

Authentication (Godkendelse) Standardindstillingen er **Auto**, som gør det muligt at bruge åben systemgodkendelse eller godkendelse med delt nøgle. Vælg **Open** (Åben) for at bruge åben systemgodkendelse, hvor afsenderen og modtageren ikke bruger en WEP-nøgle til godkendelse. Vælg **Shared** (Delt) for at bruge godkendelse med delt nøgle, hvor afsenderen og modtageren bruger en WEP-nøgle til godkendelse.

Klik på **Refresh** (Opdater) for at opdatere oplysningerne på skærmen.

Når du har angivet sikkerhedsindstillingerne, skal du klikke på **Connect** (Opret forbindelse).

Wireless (Trådløs) > WMM®

Konfigurer indstillinger for WNN (Wireless MultiMedia). WMM prioriterer pakker afhængigt af deres respektive adgangstilstand (trafiktype): Background (Baggrund), Best Effort (Bedste præstation), Video eller Voice (Tale). Indstillingerne bør kun tilpasses af en administrator med ekspertviden, da forkerte indstillinger kan forringe ydeevnen.



BEMÆRK!
Indstillingerne på skærmbilledet *WMM* er udelukkende udviklet til avancerede brugere.

WMM

Access Mode (Adgangstilstand)

Du kan konfigurere forskellige indstillinger for de fire tilgængelige adgangstilstande. Vælg den tilstand, du vil konfigurere: **Background** (Baggrund), **Best Effort** (Bedste præstation), **Video** eller **Voice** (Tale). Følg anvisningerne for den valgte tilstand.

Background (Baggrund)

Use Aggregation (Brug sammenlægning) Denne indstilling angiver, om MAC-laget (Media Access Control) opretter en ADDBA-session (Add Block Acknowledgement). Standardindstillingen er **No** (Nej). Vælg **Yes** (Ja) for at aktivere indstillingen.

Accept Aggregation (Accepter sammenlægning) Denne indstilling angiver, om MAC-laget accepterer en ADDBA-anmodning. Standardindstillingen er **Yes** (Ja). Vælg **No** (Nej) for at deaktivere indstillingen.

Max. Number of Packets in Aggregation (Maks. antal pakker i sammenlægning) Denne indstilling angiver det maksimale antal pakker (underrammer) i sammenlægningen. Intervallet er **0** til **7**. Standardindstillingen er **7**.

Max. Aggregation Size (Maks. sammenlægningsstørrelse) Denne indstilling angiver den maksimale størrelse for sammenlægningen (i byte). Intervallet er **0** til **16000**. Standardindstillingen er **12000**.

Timeout Internal (Intern timeout) Denne indstilling angiver timeoutperioden, inden for hvilken sammenlægningen skal lukkes med en "lukkebetingelse", før den lukkes af timeren. Intervallet er **0** til **100** ms. Standardindstillingen er **3**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i sammenlægning) Denne indstilling angiver den minimale størrelse (i byte) for pakker, der skal akkumuleres i sammenlægningen. Intervallet er **0** til **1500**. Standardindstillingen er **10**.

ADDBA Timeout (ADDBA-timeout) Denne indstilling angiver, hvor længe der går, før ADDBA-konfigurationen afsluttes, hvis der ikke udveksles rammepakker inden for den angivne periode med Block Acknowledgement (ACK)-aftalen. Intervallet er **0** til **65535** ms. Standardindstillingen er **0**, som deaktiverer timeoutfunktionen.

Aggregation Window Size (Størrelse på sammenlægningsvindue) Denne indstilling angiver det maksimale antal pakker, der kan overføres uden at indhente en ACK. Intervallet er **0** til **64**. Standardindstillingen er **64**.

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Best Effort (Bedste præstation)

Use Aggregation (Brug sammenlægning) Denne indstilling angiver, om MAC-laget (Media Access Control) opretter en ADDBA-session (Add Block Acknowledgement). Standardindstillingen er **Yes** (Ja). Vælg **No** (Nej) for at deaktivere indstillingen.

Accept Aggregation (Accepter sammenlægning) Denne indstilling angiver, om MAC-laget accepterer en ADDBA-anmodning. Standardindstillingen er **Yes** (Ja). Vælg **No** (Nej) for at deaktivere indstillingen.

Max. Number of Packets in Aggregation (Maks. antal pakker i sammenlægning) Denne indstilling angiver det maksimale antal pakker (underrammer) i sammenlægningen. Intervallet er **0** til **10**. Standardindstillingen er **10**.

Max. Aggregation Size (Maks. sammenlægningsstørrelse) Denne indstilling angiver den maksimale størrelse for sammenlægningen (i byte). Intervallet er **0** til **20000**. Standardindstillingen er **16000**.

Timeout Internal (Intern timeout) Denne indstilling angiver timeoutperioden, inden for hvilken sammenlægningen skal lukkes med en "lukkebetingelse", før den lukkes af timeren. Intervallet er **0** til **100** ms. Standardindstillingen er **3**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i sammenlægning) Denne indstilling angiver den minimale størrelse (i byte) for pakker, der skal akkumuleres i sammenlægningen. Intervallet er **0** til **1500**. Standardindstillingen er **10**.

ADDBA Timeout (ADDBA-timeout) Denne indstilling angiver, hvor længe der går, før ADDBA-konfigurationen afsluttes, hvis der ikke udveksles rammepakker inden for den angivne periode med Block Acknowledgement (ACK)-aftalen. Intervallet er **0** til **65535** ms. Standardindstillingen er **0**, som deaktiverer timeoutfunktionen.

Aggregation Window Size (Størrelse på sammenlægningsvindue) Denne indstilling angiver det maksimale antal pakker, der kan overføres uden at indhente en ACK. Intervallet er **0** til **64**. Standardindstillingen er **64**.

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Video

Use Aggregation (Brug sammenlægning) Denne indstilling angiver, om MAC-laget (Media Access Control) opretter en ADDBA-session (Add Block Acknowledgement). Standardindstillingen er **Yes** (Ja). Vælg **No** (Nej) for at deaktivere indstillingen.

Accept Aggregation (Accepter sammenlægning) Denne indstilling angiver, om MAC-laget accepterer en ADDBA-anmodning. Standardindstillingen er **Yes** (Ja). Vælg **No** (Nej) for at deaktivere indstillingen.

Max. Number of Packets in Aggregation (Maks. antal pakker i sammenlægning) Denne indstilling angiver det maksimale antal pakker (underrammer) i sammenlægningen. Intervallet er **0** til **7**. Standardindstillingen er **7**.

Max. Aggregation Size (Maks. sammenlægningsstørrelse) Denne indstilling angiver den maksimale størrelse for sammenlægningen (i byte). Intervallet er **0** til **16000**. Standardindstillingen er **12000**.

Timeout Internal (Intern timeout) Denne indstilling angiver timeoutperioden, inden for hvilken sammenlægningen skal lukkes med en "lukkebetingelse", før den lukkes af timeren. Intervallet er **0** til **100** ms. Standardindstillingen er **3**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i sammenlægning) Denne indstilling angiver den minimale størrelse (i byte) for pakker, der skal akkumuleres i sammenlægningen. Intervallet er **0** til **1500**. Standardindstillingen er **10**.

ADDBA Timeout (ADDBA-timeout) Denne indstilling angiver, hvor længe der går, før ADDBA-konfigurationen afsluttes, hvis der ikke udveksles rammepakker inden for den angivne periode med Block Acknowledgement (ACK)-aftalen. Intervallet er **0** til **65535** ms. Standardindstillingen er **0**, som deaktiverer timeoutfunktionen.

Aggregation Window Size (Størrelse på sammenlægningsvindue) Denne indstilling angiver det maksimale antal pakker, der kan overføres uden at indhente en ACK. Intervallet er **0** til **64**. Standardindstillingen er **64**.

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Voice (Tale)

Use Aggregation (Brug sammenlægning) Denne indstilling angiver, om MAC-laget (Media Access Control) opretter en ADDBA-session (Add Block Acknowledgement). Standardindstillingen er **Yes** (Ja). Vælg **No** (Nej) for at deaktivere indstillingen.

Accept Aggregation (Accepter sammenlægning) Denne indstilling angiver, om MAC-laget accepterer en ADDBA-anmodning. Standardindstillingen er **Yes** (Ja). Vælg **No** (Nej) for at deaktivere indstillingen.

Max. Number of Packets in Aggregation (Maks. antal pakker i sammenlægning) Denne indstilling angiver det maksimale antal pakker (underrammer) i sammenlægningen. Intervallet er **0** til **2**. Standardindstillingen er **2**.

Max. Aggregation Size (Maks. sammenlægningsstørrelse) Denne indstilling angiver den maksimale størrelse for sammenlægningen (i byte). Intervallet er **0** til **16000**. Standardindstillingen er **10000**.

Timeout Internal (Intern timeout) Denne indstilling angiver timeoutperioden, inden for hvilken sammenlægningen skal lukkes med en "lukkebetingelse", før den lukkes af timeren. Intervallet er **0** til **100** ms. Standardindstillingen er **10**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i sammenlægning) Denne indstilling angiver den minimale størrelse (i byte) for pakker, der skal akkumuleres i sammenlægningen. Intervallet er **0** til **1500**. Standardindstillingen er **10**.

ADDBA Timeout (ADDBA-timeout) Denne indstilling angiver, hvor længe der går, før ADDBA-konfigurationen afsluttes, hvis der ikke udveksles rammepakker inden for den angivne periode med Block Acknowledgement (ACK)-aftalen. Intervallet er **0** til **65535** ms. Standardindstillingen er **0**, som deaktiverer timeoutfunktionen.

Aggregation Window Size (Størrelse på sammenlægningsvindue) Denne indstilling angiver det maksimale antal pakker, der kan overføres uden at indhente en ACK. Intervallet er **0** til **64**. Standardindstillingen er **64**.

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Wireless (Trådløs) > Advanced Wireless Settings (Avancerede trådløse indstillinger)

Konfigurer de avancerede trådløse indstillinger for broen. Indstillingerne bør kun tilpasses af en administrator med ekspertviden, da forkerte indstillinger kan forringe ydeevnen.



BEMÆRK!
Indstillingerne på skærmbilledet *Advanced Wireless Settings* (Avancerede trådløse indstillinger) er udelukkende udviklet til avancerede brugere.

Advanced Wireless (Avanceret trådløs)

Use LDPC (Brug LDCP) LDCP (Low-Density Parity-Check Code) aktiverer eller deaktiverer fejlkorrektion for at reducere risikoen for datatab i kanaler med meget støj. Hastighedstilpasningsalgoritmen deaktiverer automatisk LDCP-kodning ved høje PHY-hastigheder (højere end 162). Hvis du vil bruge avanceret LDCP-fejlkorrektion, skal du bevare standardindstillingen **Yes** (Ja). Ellers skal du vælge **No** (Nej).

ERP Protection Type (ERP-beskyttelsestype) Denne indstilling konfigurerer beskyttelse af OFDM-pakker, selvom der findes 802.11b-stationer på det trådløse netværk. Ved at sende RTS/CTS- eller CTS2Self-pakker med 802.11b-hastighed informerer broen det trådløse netværk om, at der skal overføres OFDM-pakker og beskytter pakkerne på det trådløse netværk. RTS/CTS- og CTS2Self-pakkerne skaber spild, som kan resultere i lavere gennemstrømningshastigheder.

RTS/CTS-indstillingen giver bedre dækning, men lavere gennemstrømningshastigheder sammenlignet med CTS2Self, fordi RTS/CTS-indstillingen omfatter bekræftelse fra den modtagende enhed. Hvis du vil bruge RTS/CTS-indstillingen, skal du bevare standardindstillingen **RTS/CTS**. Indstillingen None (Ingen) kan forårsage kollision mellem OFDM- og CCK-pakker. Hvis du vil bruge indstillingen None (Ingen), skal du vælge **None** (Ingen). Hvis du vil bruge indstillingen CTS2Self, skal du vælge **CTS2Self**.

11n Protection Type (11n-beskyttelsestype) Denne indstilling konfigurerer beskyttelse fra ikke-HT-enheder (High Throughput) på det trådløse netværk. Hvis den trådløse router (eller adgangspunktet) registrerer, at der er enheder, som ikke understøtter HT, signalerer den til alle HT-enhederne, at de skal bruge RTS/CTS- eller CTS2Self-mekanismer forud for hver dataoverførsel. Denne funktion understøtter også alle former for 802.11n-standardbeskyttelse, herunder MIMO.

RTS/CTS-indstillingen giver bedre dækning, men lavere gennemstrømningshastigheder sammenlignet med CTS2Self, fordi RTS/CTS-indstillingen omfatter bekræftelse fra den modtagende enhed. Hvis du vil bruge RTS/CTS-indstillingen, skal du bevare standardindstillingen **RTS/CTS**. Indstillingen None (Ingen) kan forårsage kollision mellem HT-pakker og forældede pakker. Hvis du vil bruge indstillingen None (Ingen), skal du vælge **None** (Ingen). Hvis du vil bruge indstillingen CTS2Self, skal du vælge **CTS2Self**.

Percentage of maximal transmit power (Procent af maksimal effekt for afsendelse) Denne indstilling angiver procenten af den maksimale effekt for afsendelse i relation til lovbestemte domænerestriktioner. Hvis den lovbestemte domænerestriktion f.eks. tillader signalstyrker op til 20 dB, giver en indstilling på 50 % en maksimal sendeeffekt på 10 dB. Vælg den procent, du vil bruge: **12%**, **25%**, **50%** eller **100%**. Standardindstillingen er **100%**.

QoS Classification Type (QoS-klassifikationstype) Denne indstilling angiver 802.1D- eller 802.1Q-tilknytning fra feltet IP DSCP/TOS til WMM-prioriteter (Background (Baggrund), Best Effects (Bedste præstation), Video, Voice (Tale)). Bevar standardindstillingen **802.1D**, eller vælg **802.1Q**, som bruges af visse IPTV-strømme.

Re-establish Ethernet connection when initiating wireless connection (Genopret Ethernet-forbindelsen, når den trådløse forbindelse startes) Broen nulstiller Ethernet-linket mellem broen og enheden, hver gang der operettes en trådløs forbindelse, for at udløse DHCP-registrering fra den enhed, der er placeret bag ved broen. Vælg **No** (Nej) for at deaktivere denne funktionsmåde. Eller bevar standardindstillingen **Yes** (Ja).

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Administration > Management (Styring)

Brug dette skærmbillede til at styre bestemte brofunktioner: adgang til det webbaserede-hjælpeprogram, sikkerhedskopiering af konfigurationsfilen og genstart.



Management (Styring)

Bridge Access (Broadgang)

Beskyt adgangen til det browserbaserede hjælpeprogram med en adgangskode.

Bridge Password (Adgangskode for bro) Angiv en ny adgangskode for broen.

Re-enter to confirm (Gentag for at bekræfte) Indtast adgangskoden igen for at bekræfte den.

Idle Timeout (Timeout ved inaktivitet) Der opstår timeout for logonsessionen efter en bestemt periode med inaktivitet, som du angiver. Intervallet er **60** til **3600** sek. Standardindstillingen er **600**.

Web Access (Webadgang)

Access via Wireless (Adgang via trådløs) Hvis du bruger broen på et offentligt domæne, hvor du giver gæsterne trådløs adgang, kan du deaktivere trådløs adgang til broens browserbaserede hjælpeprogram. Hvis du deaktiverer indstillingen, kan du kun få adgang til det webbaserede hjælpeprogram via en kabelforbindelse. Bevar standardindstillingen **Enabled** (Aktiveret) for at tillade trådløs adgang til broens browserbaserede hjælpeprogram, eller vælg **Disabled** (Deaktiveret) for at blokere trådløs adgang til hjælpeprogrammet.

Backup and Restore (Sikkerhedskopiering og gendannelse)

Backup (Sikkerhedskopiering) Klik på **Backup Configurations** (Sikkerhedskopier konfigurationer) for at sikkerhedskopiere broens konfigurationsfil. Følg derefter anvisningerne på skærmen.

Restore (Gendannelse) Klik på **Browse** (Gennemse), og vælg konfigurationsfilen. Klik derefter på **Restore Configurations** (Gendan konfigurationer).

System Reboot (Systemgenstart)

Reboot (Genstart) Genstart broen ved at klikke på **Start to Reboot** (Start for at genstarte).

Klik på **Save Settings** (Gem indstillinger) for at anvende ændringerne, eller klik på **Cancel Changes** (Annuller ændringer) for at annullere ændringerne.

Administration > Factory Defaults (Standardindstillinger fra fabrikken)

Brug dette skærmbillede til at gendanne konfigurationen af broen til standardindstillingerne fra fabrikken.

Factory Defaults (Standardindstillinger fra fabrikken)

Restore All Settings (Gendan alle indstillinger) Klik på **Restore All Settings** (Gendan alle indstillinger) for at nulstille broens indstillinger til standardindstillingerne fra fabrikken. Eventuelle indstillinger, du har gemt, slettes, når standardindstillingerne gendannes.



Administration > Upgrade Firmware (Opgrader firmware)

Brug dette skærmbillede til at opgradere broens firmware. Opgrader kun firmwaren, hvis du har problemer med broen, eller hvis den nye firmware har en funktion, du ønsker at bruge.



Før du opgraderer firmwaren, skal du hente filen med firmwareopgraderingen til broen på Linksys-webstedet **www.Linksys.com/support**.

Upgrade Firmware (Opgrader firmware)

Please select a file to upgrade the firmware (Vælg en fil for at opgradere firmwaren) Klik på **Browse** (Gennemse), og vælg filen med firmwareopgraderingen. Klik derefter på **Start to Upgrade** (Start for at opgradere), og følg anvisningerne på skærmen.

Status > Bridge (Bro)

Der vises oplysninger om broens aktuelle status.



Bridge Information (Oplysninger om bro)

Firmware Version (Firmwareversion) Broens aktuelle firmware vises.

Local Network (Lokalt netværk)

Local MAC Address (Lokal MAC-adresse) Broens MAC-adresse på det lokale Ethernet-netværk vises.

IP Address (IP-adresse) Broens IP-adresse på det lokale Ethernet-netværk vises.

Subnet Mask (Undernetmaske) Den undernetmaske, der er konfigureret for det lokale netværk, vises.

Status > Wireless (Trådløs)

Der vises oplysninger om det trådløse netværk.



Wireless (Trådløs)

Link Status (Linkstatus) Status på forbindelsen til det trådløse netværk vises.

MAC Address (MAC-adresse) Broens MAC-adresse på det lokale trådløse netværk vises.

Network Name (SSID) (Netværksnavn (SSID)) Det trådløse netværks navn eller SSID vises.

BSSID Den trådløse MAC-adresse for den tilsluttede trådløse router (eller adgangspunktet) vises.

Radio Band (Radiobånd) Det trådløse netværks radiobånd vises.

Channel Width (Kanalbredde) Kanalbredden i MHz, som bruges af det trådløse netværk, vises.

Wide Channel (Bredkanal) Bredkanalen vises, afhængigt af kanalindstillingerne. Hvis du vælger Wide - 40MHz Channel (Bred – 40 MHz kanal) for routerens radiobånd eller kanalbredden, er dette din primære Wireless-N-kanal.

Standard Channel (Standardkanal) Indstillingen (Standardkanal) vises. Hvis du vælger Wide - 40MHz Channel (Bred – 40 MHz kanal) for routerens radiobånd eller kanalbredden, er standardkanalen din sekundære Wireless-N-kanal.

Bit Rate (Bithastighed) Dataoverførselshastigheden vises.

Signal Signalstyrken i procent vises. 100 % er den kraftigste signalstyrke, og 0 % er den svageste.

Security (Sikkerhed) Sikkerhedsmetoden for det trådløse netværk vises.

Fejlfinding

WES610N/WET610N

Computeren eller en anden kabelforbundet Ethernet-enhed kan ikke kommunikere med den trådløse router.

1. Åbn broens browserbaserede hjælpeprogram.
2. Kontroller, at netværksnavnet (SSID'et) på skærmbilledet *Basic Wireless Settings* (Grundlæggende trådløse indstillinger) svarer til navnet på det trådløse netværk.
3. Kontroller, at sikkerhedsindstillingerne (WPA, WPA2 eller WEP) svarer til sikkerhedsindstillingerne for det trådløse netværk.

Skift broens IP-adresse.

Hvis broen har forbindelse til et netværk med en DHCP-server (sædvanligvis netværksrouteren), får broen sin IP-adresse fra DHCP-serveren. Hvis der ikke er nogen DHCP-server, bruger broen den statiske IP-adresse **169.254.1.250** som standard.

Hvis du ønsker, at broen altid skal bruge en statisk IP-adresse, skal du benytte følgende fremgangsmåde:

1. Åbn broens browserbaserede hjælpeprogram.
2. Klik på fanen **Network Setup** (Netværkskonfiguration).
3. Vælg **Static IP** (Statisk IP) i rullemenuen *Network Connection Type* (Netværksforbindelsestype).
4. Udfyld felterne *Static IP Address* (Statisk IP-adresse), *Subnet Mask* (Undernetmaske) og *Default Gateway* (Standard-gateway).
5. Klik på **Save Settings** (Gem indstillinger).

En computer eller anden kabelforbundet Ethernet-enhed, som har forbindelse til broen, kan ikke kommunikere med andre enheder, hvor den trådløse funktion er aktiveret (f.eks. en computer eller printer).

Benyt følgende fremgangsmåde:

- Kontroller, at den enhed, hvor den trådløse funktion er aktiveret, er på det samme trådløse netværk som computeren eller den anden kabelforbundne Ethernet-enhed, som har forbindelse til broen.
- Kontroller, at alle enheder på det trådløse netværk bruger det samme netværksnavn (SSID).
- Kontroller, at alle enheder er på det samme IP-netværk og bruger kompatible IP-adresser.

Adgangskoden accepteres ikke af det browserbaserede hjælpeprogram.

Benyt følgende fremgangsmåde:

- Der skelnes mellem store og små bogstaver i adgangskoden. Kontroller, at du skriver bogstaverne korrekt med stort og småt, når du indtaster adgangskoden.
- Hvis du glemmer din adgangskode, kan du nulstille broen til standardindstillingerne fra fabrikken.

 Tryk på **nulstillingsknappen** på broen, og og hold den inde i ca. frem sekunder. Adgangskoden nulstilles til standardindstillingen **admin**. Alle andre indstillinger for broen nulstilles også til standardindstillingerne fra fabrikken. Du kan få adgang til det browserbaserede hjælpeprogram ved at skrive **admin** i feltet *Password* (Adgangskode).

De nye indstillinger vises ikke på skærmen, når du foretager ændringer via det browserbaserede hjælpeprogram.

Klik på **Refresh** (Opdater) i webbrowseren. Benyt følgende fremgangsmåde, hvis de nye indstillinger ikke vises:

1. Fjern strømadapteren fra broen.
2. Vent fem sekunder, og slut derefter strømadapteren til broen igen.
3. Klik på **Refresh** (Opdater) i webbrowseren.

INTERNETTET
Hvis dit spørgsmål ikke er angivet her, kan du finde flere oplysninger på Linksys-webstedet på **Linksys.com/support**

Specifikationer

WES610N

Model	WES610N
Standarder	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Indikatorer	Strøm, Ethernet, Wi-Fi Protected Setup™, Trådløs, individuelt Ethernet-link og aktivitet
Porte	Ethernet (4), Strøm
Knapper	Reset (Nulstil), Wi-Fi Protected Setup
Kabeltype	CAT5e
Antenner	3 (interne)
Antennestiktype	Ikke tilgængelig
Aftagelig (Ja/Nej)	Nej
Modulationer	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) i dBm	802.11a: 15 dBm (typisk) ved 54 Mbps 802.11b: 19 dBm (typisk) ved 11 Mbps 802.11g: 16 dBm (typisk) ved 54 Mbps 802.11n (2,4 GHz): 18 dBm (typisk) ved MCS15 802.11n (5 GHz): 16 dBm (typisk) ved MCS15
Modtagefølsomhed	802.11a: -72 dBm (typisk) ved 54 Mbps 802.11b: -85 dBm (typisk) ved 11 Mbps 802.11g: -73 dBm (typisk) ved 54 Mbps 802.11n (20 MHz): -75 dBm (typisk) ved MCS15 802.11n (40 MHz): -69 dBm (typisk) ved MCS15
Antenneforstærkning i dBi	1
Trådløs sikkerhed	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Sikkerhedsnøglebit	Op til 128-bit kryptering

Miljø

Mål	6,97" x 5,04" x 2,68" (177 x 128 x 68 mm)
Vægt	0,65 lb (295 g)
Certificering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Strøm	12 V, 1 A
Driftstemperatur	32 til 104º F (0 til 40º C)
Opbevaringstemperatur	-4 til 140º F (-20 til 60º C)
Luftfugtighed ved drift	10 til 85 %, ingen kondensering
Luftfugtighed ved opbevaring	5 til 90 %, ingen kondensering

Specifikationer kan ændres uden varsel.

WET610N

Model	WET610N
Standarder	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Indikatorer	Strøm, Ethernet, Wi-Fi Protected Setup™, Wireless
Porte	Ethernet, Strøm
Knapper	Reset (Nulstil), Wi-Fi Protected Setup
Kabeltype	CAT5e
Antenner	3 (interne)
Antennestiktype	Ikke tilgængelig
Aftagelig (Ja/Nej)	Nej
Modulationer	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) i dBm	802.11a: 15 dBm (typisk) ved 54 Mbps 802.11b: 18 dBm (typisk) ved 11 Mbps 802.11g: 16 dBm (typisk) ved 54 Mbps 802.11n: 12 dBm (typisk) ved 130 Mbps (HT20), 270 Mbps (HT40)
Modtagefølsomhed	802.11a: -72 dBm (typisk) ved 54 Mbps 802.11b: -85 dBm (typisk) ved 11 Mbps 802.11g: -73 dBm (typisk) ved 54 Mbps 802.11n: -70 dBm (typisk) ved MCS15/2.4 GHz, -69 dBm (typisk) ved MCS15/5.0 GHz
Antenneforstærkning i dBi	1
Trådløs sikkerhed	WEP, WPA (Wi-Fi Protected Access™), WPA2 (Wi-Fi Protected Access™ 2)
Sikkerhedsnøglebit	Op til 128-bit kryptering

Miljø

Mål	5,71" x 4,17" x 2,05" (145 x 106 x 52 mm)
Vægt	5,61 oz (159 g)
Certificering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Strøm	12 V, 1 A
Driftstemperatur	32 til 104º F (0 til 40º C)
Opbevaringstemperatur	-4 til 140º F (-20 til 60º C)
Luftfugtighed ved drift	10 til 85 %, ingen kondensering
Luftfugtighed ved opbevaring	5 til 90 %, ingen kondensering

Specifikationer kan ændres uden varsel.

Linksys.com/support

Cisco, Cisco-logoet og Linksys er varemærker eller registrerede varemærker tilhørende Cisco og/eller Ciscos tilknyttede virksomheder i USA og andre lande.
En liste over Ciscos varemærker findes på www.cisco.com/go/trademarks. Alle andre varemærker, som nævnes i dette dokument, tilhører de respektive ejere.

© 2011 Cisco og/eller Ciscos tilknyttede virksomheder. Alle rettigheder forbeholdes.

3425-01249



Guía del usuario

Linksys WET610N/WES610N | Puente de ocio con doble banda N

Contenido

Descripción del producto

Panel de luz 2
Panel de puertos 3

Lista de comprobación de seguridad inalámbrica

Cambie el SSID o nombre predeterminado de la red inalámbrica 4
Cambie la contraseña predeterminada 4
Active el filtrado de direcciones MAC 4
Active la encriptación 4
Directrices generales de seguridad de la red 4
Sugerencias de seguridad adicionales 5

Configuración avanzada

Cómo acceder a la utilidad basada en explorador 6
Setup > Basic Setup (Configuración > Configuración básica) . . . 7
Language (Idioma) 7
Network Setup (Configuración de red) 7
Wireless > Basic Wireless Settings (Inalámbrico > Parámetros inalámbricos básicos) 7
Basic Wireless Settings (Parámetros inalámbricos básicos) 8
Wireless Security (Seguridad inalámbrica) 8
Wi-Fi Protected Setup (Configuración Wi-Fi protegida) 9
Wireless > Wireless Network Site Survey (Inalámbrico > Sondeo del sitio inalámbrico) 10
Wireless Network Site Survey (Sondeo del sitio inalámbrico) 10
Wireless > WMM® (Inalámbrico > WMM®) 11
WMM 12
Wireless > Advanced Wireless Settings (Inalámbrico > Parámetros inalámbricos avanzados) 13
Advanced Wireless (Parámetros inalámbricos avanzados) 14
Administration > Management (Administración > Gestión) . . . 14
Management (Gestión) 14
Administration > Factory Defaults (Administración > Parámetros predeterminados de fábrica) 15
Factory Defaults (Parámetros predeterminados de fábrica) 15
Administration > Upgrade Firmware (Administración > Actualizar el firmware) 15
Upgrade Firmware (Actualizar el firmware) 15
Status > Bridge (Estado > Puente) 15
Bridge Information (Información del puente) 16
Local Network (Red local) 16
Status > Wireless (Estado > Inalámbrica) 16
Wireless (Inalámbrico) 16

Resolución de problemas

WES610N/WET610N 17

Especificaciones

WES610N 18
WET610N 19

Descripción del producto

Gracias por elegir el puente de ocio de doble banda N de Linksys. El puente es capaz de conectar cualquier dispositivo Ethernet con cables a la red inalámbrica. El puente se basa en Wireless-N de doble banda, por lo que es compatible con cualquier router o punto de acceso Wireless-N, -G, -A, o -B. Para la instalación inicial, siga los pasos que se indican en la carpeta del CD. Para configurar los parámetros avanzados, utilice la práctica utilidad basada en explorador.

Panel de luz



WES610N WET610N

Conexión inalámbrica (azul) Se enciende cuando existe una conexión inalámbrica. La luz parpadea cuando el puente envía o recibe datos de forma activa a través de la red inalámbrica.

Botón de configuración Wi-Fi protegida Si el router es compatible con la configuración Wi-Fi protegida y utiliza seguridad WPA o WPA2, puede utilizar la Configuración Wi-Fi protegida para conectar el puente de forma automática. Para utilizar la configuración Wi-Fi protegida, consulte "Wireless > Basic Wireless Settings (Inalámbrico > Parámetros inalámbricos básicos)" en la página 7.

Luz de configuración Wi-Fi protegida (azul/ámbar) Parpadea en azul durante dos minutos en la configuración Wi-Fi protegida. Se ilumina en azul cuando se activa la seguridad inalámbrica. Si se produce un error durante el proceso de-configuración Wi-Fi protegida, la luz se ilumina en ámbar. Asegúrese de que el router de la red es compatible con la-configuración Wi-Fi protegida. Espere a que la luz se apague y vuelva a intentarlo.

Ethernet (azul) La luz Ethernet se ilumina cuando existe una conexión con cables y parpadea cuando el puente envía o recibe datos de forma activa a través del puerto Ethernet.

Alimentación (azul) El indicador de alimentación se ilumina cuando el puente está encendido.

Panel de puertos



WES610N WET610N

Ethernet El puerto Ethernet conecta el puente a un equipo o a otro dispositivo de red Ethernet. El WES610N dispone de cuatro puertos y el WET610N dispone de un único puerto.

Reinicio Hay dos formas de restablecer los parámetros predeterminados de fábrica del puente. Pulse el botón de reinicio durante unos cinco segundos o restaure los parámetros predeterminados desde Administration > Factory Defaults (Administración > Parámetros predeterminados de fábrica) en la utilidad basada en explorador del puente. El WES610N dispone de un botón de reinicio en la parte inferior y el WET610N dispone de un botón de reinicio en el panel del puerto posterior.

Power (Alimentación) Este puerto conecta el puente al adaptador de corriente incluido.

Lista de comprobación de seguridad inalámbrica

Las redes inalámbricas son prácticas y fáciles de instalar, por lo que el número de hogares que están instalando un acceso a Internet de alta velocidad está creciendo rápidamente. Puesto que las redes inalámbricas funcionan enviando información a través de las ondas de radio, pueden ser más vulnerables frente a los intrusos que una red con cables tradicional. Al igual que las señales que emiten los teléfonos móviles o inalámbricos, las señales de la red inalámbrica también se pueden interceptar. Dado que no se puede prevenir físicamente que alguien se conecte a su red inalámbrica, deberá tomar algunas medidas adicionales para mantener la seguridad de la red.

Cambie el SSID o nombre predeterminado de la red inalámbrica

Los dispositivos inalámbricos tienen un nombre de red inalámbrica o identificador del conjunto de servicios (SSID) predeterminado y configurado de fábrica. Éste es el nombre de su red inalámbrica y puede tener una longitud de hasta 32 caracteres. Los productos inalámbricos de Linksys utilizan **linksys** como nombre predeterminado de la red inalámbrica. Debe cambiar el nombre de la red inalámbrica a alguno exclusivo que distinga su red de otras redes inalámbricas que puedan existir cerca, pero no utilice información personal (como el número de la seguridad social o el DNI) porque esta información podría estar disponible para cualquier persona que busque redes inalámbricas.

Cambie la contraseña predeterminada

Se le solicitará una contraseña cuando desee modificar los parámetros de los productos inalámbricos como puntos de acceso y routers. Estos dispositivos tienen una contraseña predeterminada configurada de fábrica. La contraseña predeterminada de Linksys es **admin**. Los hackers conocen estas contraseñas predeterminadas y podrían intentar utilizarlas para obtener acceso a su dispositivo inalámbrico y cambiar los parámetros de la red. Para evitar los cambios no autorizados, personalice la contraseña del dispositivo para que resulte difícil de adivinar.

Active el filtrado de direcciones MAC

Los routers de Linksys le permiten activar el filtrado de direcciones MAC (control de acceso a medios). La dirección MAC es una serie única de números y letras que se asigna a cada dispositivo de red. Con el filtrado de direcciones MAC activado, sólo se proporcionará acceso a la red inalámbrica a los dispositivos inalámbricos con direcciones MAC específicas. Por ejemplo, puede especificar la dirección MAC de cada computadora de su hogar para que sólo ellos puedan acceder a su red inalámbrica.

Active la encriptación

La encriptación protege los datos que se transmiten a través de una red inalámbrica. El acceso Wi-Fi protegido (WPA/WPA2) y la privacidad equivalente a conexión con cables (WEP) ofrecen varios niveles de seguridad para la comunicación inalámbrica.

Una red encriptada con WPA/WPA2 es más segura que una red encriptada con WEP porque WPA/WPA2 utiliza una encriptación de clave dinámica. Para proteger la información cuando se transmite a través de las ondas, deberá activar el nivel más alto de encriptación que admita el equipo de red.

WEP es un estándar de encriptación antiguo y puede ser la única opción disponible en algunos dispositivos que no admitan WPA.

Directrices generales de seguridad de la red

La seguridad de la red inalámbrica no sirve de nada si la red subyacente no es segura.

- Con una contraseña, se pueden proteger todas las computadoras de la red y, con una contraseña individual, se pueden proteger los archivos confidenciales.
- Cambie las contraseñas de forma regular.
- Instale un software antivirus y un software de firewall personal.
- Desactive el intercambio de archivos (de igual a igual). Algunas aplicaciones pueden activar el intercambio de archivos sin su consentimiento o conocimiento.

Sugerencias de seguridad adicionales

- Mantenga los puntos de acceso, las gateways o los routers inalámbricos alejados de paredes exteriores y ventanas.
- Apague los puntos de acceso, las gateways o los routers inalámbricos cuando no los esté utilizando (por la noche y durante las vacaciones).
- Utilice frases de paso seguras que tengan una longitud mínima de ocho caracteres. Combine letras y números para evitar el uso de palabras estándar que puedan encontrarse en un diccionario.

Configuración avanzada

Después de configurar el puente siguiendo los pasos que se indican en la carpeta del CD, el puente estará listo para utilizarse. Sin embargo, si desea cambiar su configuración avanzada, utilice la utilidad basada en explorador del puente. En este capítulo se describen las páginas web de la utilidad y las funciones clave de cada una. Puede acceder a la utilidad mediante el explorador web de un ordenador que esté conectado en red al puente.

La utilidad basada en explorador cuenta con las siguientes fichas principales: Setup (Configuración), Wireless (Inalámbrico), Administration (Administración) y Status (Estado). Al hacer clic en una de las fichas principales, aparecerán fichas adicionales.

Cómo acceder a la utilidad basada en explorador

Utilice un explorador web para acceder a la utilidad basada en explorador.

Si el puente está conectado a una red con un servidor DHCP (normalmente el router de la red), el puente utilizará el servidor DHCP para obtener su dirección IP. Si no hay un servidor DHCP, el puente utilizará la dirección IP estática predeterminada: **169.254.1.250**. (Si configura una dirección IP estática permanente en el puente mediante la utilidad basada en explorador, introduzca la dirección IP estática en su lugar).

NOTA
Si no conoce la dirección IP del puente, búsquela en la tabla de clientes DHCP del router. (Consulte la documentación del router).

Si no encuentra la dirección IP del puente, puede reiniciarlo. Para ello, pulse el botón de **reinicio** con un clip de papel recto durante cinco segundos aproximadamente. De este modo, el puente volverá a tener la parámetros predeterminados de fábrica. El puente solicitará una dirección IP al servidor DHCP (normalmente el router de la red). Si no se encuentra un servidor DHCP, el puente utilizará la dirección IP estática predeterminada, **169.254.1.250**, hasta que detecte un servidor DHCP y se le asigne una dirección IP dinámica.

Si el puente no está asociado a un router y utiliza los parámetros predeterminados de fábrica, conecte un ordenador al puente a través de una conexión Ethernet para acceder a la utilidad basada en web. Necesitará configurar la conexión Ethernet del ordenador con una dirección IP estática y una máscara de subred.

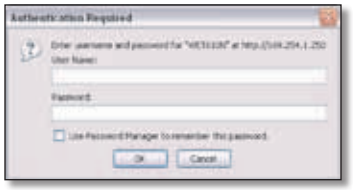
La dirección IP del adaptador Ethernet debería establecerse como una dirección IP específica.

1. En el campo *IP address* (Dirección IP), introduzca **169.254.x.y** (donde x debe sustituirse por un número entre 1 y 254 e y por un número entre 0 y 255).
2. En el campo *Subnet mask* (Máscara de subred), introduzca **255.255.0.0**.

NOTA
Los pasos para asignar una dirección IP estática al adaptador Ethernet del ordenador varían según el sistema operativo. Para obtener más instrucciones, consulte la documentación de ayuda para el sistema operativo específico de su ordenador.

Después de asignar una dirección IP estática al adaptador Ethernet, abra el explorador web e introduzca la dirección IP del adaptador (el valor predeterminado es **169.254.1.250**) en el campo *Address* (Dirección). Pulse **Intro**.

A continuación, aparece una pantalla en la que se le solicita una contraseña. (Si no es usuario de Windows XP verá una pantalla parecida). Deje el campo *User Name* (Nombre de usuario) en blanco. Introduzca la contraseña creada durante la ejecución del asistente de configuración. Si no creó una nueva contraseña, utilice la contraseña predeterminada **admin**. (Puede establecer una nueva contraseña en la pantalla *Administration* > *Management* [Administración > Gestión]). Haga clic en **OK** (Aceptar) para continuar.



NOTA
Si no aparece la pantalla en la que se le solicita la contraseña, espere dos minutos y vuelva a intentarlo.

Setup > Basic Setup (Configuración > Configuración básica)

La primera pantalla que aparece es *Basic Setup* (Configuración básica). Utilice esta pantalla para cambiar el idioma de la utilidad basada en explorador o para modificar los parámetros de red Ethernet y con cables del puente.





Language (Idioma)

Language (Idioma) Esta opción se utiliza para establecer el idioma que se mostrará en la utilidad basada en explorador. Seleccione el idioma que desee en el menú desplegable.

Network Setup (Configuración de red)

Esta sección determina si la dirección IP del puente se obtiene de forma automática desde un servidor DHCP, como hace un router de red (Configuración automática - DHCP), o de forma manual (IP estática).

Bridge IP (Dirección IP del puente) Si su red cuenta con servidor DHCP como, por ejemplo, un router de red que asigna las direcciones IP a los dispositivos de red, mantenga el valor predeterminado **Automatic Configuration - DHCP** (Configuración automática - DHCP). El puente solicitará una dirección IP al servidor DHCP (normalmente el router de la red). Si no se encuentra un servidor DHCP, el puente utilizará la dirección IP estática predeterminada, **169.254.1.250**, hasta que detecte un servidor DHCP y se le asigne una dirección IP dinámica.

Si desea establecer una dirección IP estática permanente para el puente, seleccione **Static IP** (IP estática).

En este caso, rellene los siguientes campos:

- **Static IP Address** (Dirección IP estática) Introduzca una dirección IP única que se utilizará para acceder a la utilidad basada en explorador.
- **Subnet Mask** (Máscara de subred) Introduzca la cámara de subred de la red con cables.
- **Default Gateway** (Gateway predeterminada) Introduzca la dirección IP de la gateway predeterminada para la red (la mayoría de las veces, es el router).

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Wireless > Basic Wireless Settings (Inalámbrico > Parámetros inalámbricos básicos)

Utilice la pantalla *Basic Wireless Settings* (Parámetros inalámbricos básicos) para configurar los parámetros inalámbricos básico y de seguridad del puente.

Hay dos formas de configurar los parámetros del puente: la configuración manual y la configuración Wi-Fi protegida. La configuración Wi-Fi protegida es una función que facilita la configuración de la red inalámbrica. Si el router de la red es compatible con la configuración Wi-Fi protegida y emplea seguridad WPA o WPA2, puede utilizar la configuración Wi-Fi protegida para conectar el puente de forma automática.

Configuration View (Vista de configuración) Para configurar una red inalámbrica de manera manual, seleccione **Manual**. Consulte **Basic Wireless Settings** (Parámetros inalámbricos básicos), **página 8**. Para utilizar la configuración Wi-Fi protegida, seleccione **Wi-Fi Protected Setup** (Configuración Wi-Fi protegida). Consulte **Wi-Fi Protected Setup** (Configuración Wi-Fi protegida), **página 9**.

Basic Wireless Settings (Parámetros inalámbricos básicos)



Network Name (SSID) (Nombre de la red, SSID) El SSID es el nombre de red que comparten todos los puntos de una red inalámbrica. Debe ser el mismo para todos los dispositivos de la red inalámbrica. El nombre distingue entre mayúsculas y minúsculas y no debe tener una longitud superior a los 32 caracteres (se puede utilizar cualquier carácter del teclado). Compruebe que este parámetro coincide con el parámetro del router inalámbrico o el punto de acceso. Para mayor seguridad, debe cambiar el SSID predeterminado (**linksys**) por otro que sea exclusivo.

Wireless Security (Seguridad inalámbrica)

El puente es compatible con las siguientes opciones de seguridad inalámbrica: WPA Personal, WPA2 Personal y WEP. WPA (Acceso Wi-Fi protegido) y WPA2 son métodos de seguridad más fiables que WEP (Privacidad equivalente a conexión con cables). Para obtener más información sobre la seguridad inalámbrica, consulte "Lista de comprobación de seguridad inalámbrica", página 4.

Security Mode (Modo de seguridad)

Seleccione el método de seguridad para la red inalámbrica. Si no desea utilizar la seguridad inalámbrica, mantenga el parámetro predeterminado **Disabled** (Desactivado).

NOTA
Recuerde que todos los dispositivos de la red inalámbrica DEBEN utilizar el mismo método de seguridad y frase de paso/clave. De lo contrario, no podrán comunicarse entre sí.

WPA Personal

WPA es un estándar de seguridad más fiable que la encriptación WEP.



Encryption (Encriptación) WPA es compatible con el método de encriptación TKIP, que cuenta con claves de encriptación dinámica.

Passphrase (Frase de paso) Introduzca la clave compartida por el puente y el router inalámbrico o el punto de acceso. Debe tener entre 8 y 63 caracteres.

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

WPA2 Personal

WPA2 es una versión más avanzada y segura de WPA.



Encryption (Encriptación) WPA2 es compatible con dos métodos de encriptación, TKIP y AES, con claves de encriptación dinámica. Seleccione el tipo de encriptación, **AES** o **bien TKIP o AES**. La selección predeterminada es **AES**.

Passphrase (Frase de paso) Introduzca la clave compartida por el puente y el router inalámbrico o el punto de acceso. Debe tener entre 8 y 63 caracteres.

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

WEP

WEP es un método de encriptación básico y no es tan seguro como WPA o WPA2.



Encryption (Encriptación) Seleccione un nivel de encriptación WEP **40/64 bits (10 hex digits)** (40/64 bits, 10 dígitos hexadecimales) o **104/128 bits (26 hex digits)** (104/128 bits, 26 dígitos hexadecimales). El valor predeterminado es **40/64 bits (10 hex digits)** (40/64 bits, 10 dígitos hexadecimales).

Key 1 (Clave 1) Introduzca la clave WEP de la red.

Tx Key (Clave de transmisión) **Key 1** es la clave de transmisión utilizada por el puente.

Authentication (Autenticación) El valor predeterminado es **Auto** (Automático), que permite utilizar la autenticación Open System (Sistema abierto) o Shared key (Clave compartida). Seleccione **Open** (Abierto) para utilizar la autenticación de sistema abierto, en la que el emisor y el receptor no utilizan una clave WEP para la autenticación. Seleccione **Shared** (Compartida) para utilizar la autenticación de clave compartida, en la que el emisor y el receptor utilizan una clave WEP para la autenticación.

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Wi-Fi Protected Setup (Configuración Wi-Fi protegida)

Hay dos métodos disponibles. Utilice el método que corresponda al router que está utilizando.





Método 1

Utilice este método si el router tiene un botón de configuración Wi-Fi protegida.

1. Haga clic o pulse el botón de **configuración Wi-Fi protegida** del router.
2. Al cabo de dos minutos, pulse el botón de **configuración Wi-Fi protegida** que aparece en la pantalla *Wi-Fi Protected Setup* (Configuración Wi-Fi protegida) del puente.
3. Una vez que haya configurado el puente, haga clic en **Close** (Cerrar).

La pantalla *Wi-Fi Protected Setup* (Configuración Wi-Fi protegida) muestra el estado de la conexión, el nombre de red (SSID) y el método de seguridad.

Método 2

Utilice este método si el router solicita el número PIN del puente.

1. En la **pantalla** *Wi-Fi Protected Setup* (Configuración Wi-Fi protegida) del router, introduzca el número PIN que aparece en la **pantalla** *Wi-Fi Protected Setup* (Configuración Wi-Fi protegida) del puente. A continuación, haga clic en **Register** (Registro) o en el botón adecuado. (También aparece en la etiqueta de la parte inferior del puente).
2. En la **pantalla** *Wi-Fi Protected Setup* (Configuración Wi-Fi protegida), haga clic en **OK** (Aceptar).
3. Una vez que haya configurado el puente, haga clic en **Close** (Cerrar).

La pantalla *Wi-Fi Protected Setup* (Configuración Wi-Fi protegida) muestra el estado de la conexión, el nombre de red (SSID) y el método de seguridad.

Wireless > Wireless Network Site Survey (Inalámbrico > Sondeo del sitio inalámbrico)

Haga clic en la ficha **Wireless Network Site Survey** (Sondeo del sitio inalámbrico) para comenzar un sondeo del sitio. La pantalla *Wireless Network Site Survey* (Sondeo del sitio inalámbrico) muestra las redes inalámbricas que ha detectado el puente.



Wireless Network Site Survey (Sondeo del sitio inalámbrico)

Number of Wireless Networks (Número de redes inalámbricas) Muestra el número de redes inalámbricas que ha detectado el puente.

Select (Seleccionar) Para conectarse a una red inalámbrica, haga clic en **Select** (Seleccionar). A continuación, haga clic en **Connect** (Conectar).

Wireless Network Name (Nombre de la red inalámbrica) Muestra el nombre de la red o SSID de la red inalámbrica.

GHz Muestra la banda de radio de la red inalámbrica.

Signal (Señal) Muestra el porcentaje de la potencia de la señal. La potencia máxima de la señal es 100% y la mínima, 0%.

Security (Seguridad) Si la red es compatible con la configuración WiFi protegida, se muestra el icono de configuración Wi-Fi protegida . Además, se muestra el método de seguridad que utiliza la red inalámbrica.

Haga clic en el botón de **actualización** para actualizar la información de la pantalla.

Cuando haya seleccionado una red, haga clic en **Connect** (Conectar). Aparecerá una nueva pantalla. Siga las instrucciones del método de seguridad de la red.

WPA



Network Name (SSID) (Nombre de la red, SSID) Muestra automáticamente el nombre de la red que ha seleccionado.

Security Mode (Modo de seguridad) Aparece automáticamente el modo WPA Personal.

Encryption (Encriptación) WPA es compatible con el método de encriptación TKIP, que cuenta con claves de encriptación dinámica.

Passphrase (Frase de paso) Introduzca la clave compartida por el puente y el router inalámbrico o el punto de acceso. Debe tener entre 8 y 63 caracteres.

Haga clic en el botón de **actualización** para actualizar la información de la pantalla.

Cuando haya introducido los parámetros de seguridad, haga clic en **Connect** (Conectar).

WPA2



Network Name (SSID) (Nombre de la red, SSID) Muestra automáticamente el nombre de la red que ha seleccionado.

Security Mode (Modo de seguridad) Aparece automáticamente el modo WPA2 Personal.

Encryption (Encriptación) WPA2 es compatible con dos métodos de encriptación, TKIP y AES, con claves de encriptación dinámica. Seleccione el tipo de encriptación, **AES** o **bien TKIP or AES** (TKIP o AES).

Passphrase (Frase de paso) Introduzca la clave compartida por el puente y el router inalámbrico o el punto de acceso. Debe tener entre 8 y 63 caracteres.

Haga clic en el botón de **actualización** para actualizar la información de la pantalla.

Cuando haya introducido los parámetros de seguridad, haga clic en **Connect** (Conectar).

WEP



Network Name (SSID) (Nombre de la red, SSID) Muestra automáticamente el nombre de la red que ha seleccionado.

Security Mode (Modo de seguridad) Aparece automáticamente el modo WEP.

Encryption (Encriptación) Seleccione un nivel de encriptación WEP, **40/64 bits (10 hex digits)** (40/64 bits, 10 dígitos hexadecimales) o **104/128 bits (26 hex digits)** (104/128 bits, 26 dígitos hexadecimales).

Key 1 (Clave 1) Introduzca la clave WEP de la red.

Tx Key (Clave de transmisión) **Key 1** es la clave de transmisión utilizada por el puente.

Authentication (Autenticación) El valor predeterminado es **Auto** (Automático), que permite utilizar la autenticación Open System (Sistema abierto) o Shared key (Clave compartida). Seleccione **Open** (Abierto) para utilizar la autenticación de sistema abierto, en la que el emisor y el receptor no utilizan una clave WEP para la autenticación. Seleccione **Shared** (Compartida) para utilizar la autenticación de clave compartida, en la que el emisor y el receptor utilizan una clave WEP para la autenticación.

Haga clic en el botón de **actualización** para actualizar la información de la pantalla.

Cuando haya introducido los parámetros de seguridad, haga clic en **Connect** (Conectar).

Wireless > WMM® (Inalámbrico > WMM®)

Configure los parámetros Wireless MultiMedia (WMM). WMM da prioridad a los paquetes en función de su modo de acceso (tipo de tráfico): Background (Fondo), Best Effort (Mayor esfuerzo), Video (Vídeo) o Voice (Voz). Estos parámetros sólo los debe ajustar un administrador experto, ya que unos parámetros incorrectos pueden reducir el rendimiento inalámbrico.



NOTA
Los parámetros que aparecen en la pantalla *WMM* están dirigidos a usuarios avanzados.

WMM

Access Mode (Modo de acceso)

Puede asignar diferentes parámetros a los cuatro modos de acceso disponibles. Seleccione el modo que desea utilizar. **Background** (Fondo), **Best Effort** (Mayor esfuerzo), **Video** (Vídeo), o **Voice** (Voz). Siga las instrucciones del modo que haya seleccionado.

Background (Fondo)

Use Aggregation (Utilizar adición) Esta opción establece si la capa MAC (Control de acceso a medios) configurará una sesión ADDBA (Agregar confirmación de bloque). El valor predeterminado es **No**. Seleccione **Yes** (Sí) para activar esta opción.

Accept Aggregation (Aceptar adición) Esta opción indica si la capa MAC aceptará una solicitud ADDBA. El valor predeterminado es **Yes** (Sí). Seleccione **No** para desactivar esta opción.

Number of Packets in Aggregation (Número máximo de paquetes en adición) Esta opción indica el número máximo de paquetes (subtramas) de la adición. El intervalo es de **0** a **7**. El valor predeterminado es **7**.

Max. Aggregation Size (Tamaño máximo de adición) Esta opción indica el tamaño máximo de la adición (en bytes). El intervalo es de **0** a **16.000**. El valor predeterminado es **12.000**.

Timeout Interval (Tiempo de espera) Esta opción indica, mediante una "condición de cierre", el tiempo de espera en el que la adición debe finalizar antes de que el temporizador la cierre. El intervalo es de **0** a **100** ms. El valor predeterminado es **3**.

Size of Packet in Aggregation (Tamaño mínimo de paquetes en adición) Esta opción indica el tamaño mínimo (en bytes) de los paquetes acumulados durante la adición. El intervalo es de **0** a **1.500**. El valor predeterminado es **10**.

ADDBA Timeout (Tiempo de espera ADDBA) Esta opción indica el periodo de tiempo tras el que finaliza la configuración ADDBA, si en ese tiempo no se realiza intercambio de tramas según el acuerdo ACK (Confirmación de bloque). El intervalo es de **0** a **65.535** ms. El valor predeterminado es **0**, que desactiva la función de tiempo de espera.

Aggregation Window Size (Tamaño de la ventana de adición) Esta opción indica el número máximo de paquetes que se han transmitido sin confirmación de bloque. El intervalo es de **0** a **64**. El valor predeterminado es **64**.

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Best Effort (Mayor esfuerzo)

Use Aggregation (Utilizar adición) Esta opción establece si la capa MAC (Control de acceso a medios) configurará una sesión ADDBA (Agregar confirmación de bloque). El valor predeterminado es **Yes** (Sí). Seleccione **No** para desactivar esta opción.

Accept Aggregation (Aceptar adición) Esta opción indica si la capa MAC aceptará una solicitud ADDBA. El valor predeterminado es **Yes** (Sí). Seleccione **No** para desactivar esta opción.

Number of Packets in Aggregation (Número máximo de paquetes en adición) Esta opción indica el número máximo de paquetes (subtramas) de la adición. El intervalo es de **0** a **10**. El valor predeterminado es **10**.

Max. Aggregation Size (Tamaño máximo de adición) Esta opción indica el tamaño máximo de la adición (en bytes). El intervalo es de **0** a **20.000**. El valor predeterminado es **16.000**.

Timeout Interval (Tiempo de espera) Esta opción indica, mediante una "condición de cierre", el tiempo de espera en el que la adición debe finalizar antes de que el temporizador la cierre. El intervalo es de **0** a **100** ms. El valor predeterminado es **3**.

Size of Packet in Aggregation (Tamaño mínimo de paquetes en adición) Esta opción indica el tamaño mínimo (en bytes) de los paquetes acumulados durante la adición. El intervalo es de **0** a **1.500**. El valor predeterminado es **10**.

ADDBA Timeout (Tiempo de espera ADDBA) Esta opción indica el periodo de tiempo tras el que finaliza la configuración ADDBA, si en ese tiempo no se realiza intercambio de tramas según el acuerdo ACK (Confirmación de bloque). El intervalo es de **0** a **65.535** ms. El valor predeterminado es **0**, que desactiva la función de tiempo de espera.

Aggregation Window Size (Tamaño de la ventana de adición) Esta opción indica el número máximo de paquetes que se han transmitido sin confirmación de bloque. El intervalo es de **0** a **64**. El valor predeterminado es **64**.

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Video (Vídeo)

Use Aggregation (Utilizar adición) Esta opción establece si la capa MAC (Control de acceso a medios) configurará una sesión ADDBA (Agregar confirmación de bloque). El valor predeterminado es **Yes** (Sí). Seleccione **No** para desactivar esta opción.

Accept Aggregation (Aceptar adición) Esta opción indica si la capa MAC aceptará una solicitud ADDBA. El valor predeterminado es **Yes** (Sí). Seleccione **No** para desactivar esta opción.

Number of Packets in Aggregation (Número máximo de paquetes en adición) Esta opción indica el número máximo de paquetes (subtramas) de la adición. El intervalo es de **0** a **7**. El valor predeterminado es **7**.

Max. Aggregation Size (Tamaño máximo de adición) Esta opción indica el tamaño máximo de la adición (en bytes). El intervalo es de **0** a **16.000**. El valor predeterminado es **12.000**.

Timeout Interval (Tiempo de espera) Esta opción indica, mediante una "condición de cierre", el tiempo de espera en el que la adición debe finalizar antes de que el temporizador la cierre. El intervalo es de **0** a **100** ms. El valor predeterminado es **3**.

Size of Packet in Aggregation (Tamaño mínimo de paquetes en adición) Esta opción indica el tamaño mínimo (en bytes) de los paquetes acumulados durante la adición. El intervalo es de **0** a **1.500**. El valor predeterminado es **10**.

ADDBA Timeout (Tiempo de espera ADDBA) Esta opción indica el periodo de tiempo tras el que finaliza la configuración ADDBA, si en ese tiempo no se realiza intercambio de tramas según el acuerdo ACK (Confirmación de bloque). El intervalo es de **0** a **65.535** ms. El valor predeterminado es **0**, que desactiva la función de tiempo de espera.

Aggregation Window Size (Tamaño de la ventana de adición) Esta opción indica el número máximo de paquetes que se han transmitido sin confirmación de bloque. El intervalo es de **0** a **64**. El valor predeterminado es **64**.

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Voice (Voz)

Use Aggregation (Utilizar adición) Esta opción establece si la capa MAC (Control de acceso a medios) configurará una sesión ADDBA (Agregar confirmación de bloque). El valor predeterminado es **Yes** (Sí). Seleccione **No** para desactivar esta opción.

Accept Aggregation (Aceptar adición) Esta opción indica si la capa MAC aceptará una solicitud ADDBA. El valor predeterminado es **Yes** (Sí). Seleccione **No** para desactivar esta opción.

Number of Packets in Aggregation (Número máximo de paquetes en adición) Esta opción indica el número máximo de paquetes (subtramas) de la adición. El intervalo es de **0** a **2**. El valor predeterminado es **2**.

Max. Aggregation Size (Tamaño máximo de adición) Esta opción indica el tamaño máximo de la adición (en bytes). El intervalo es de **0** a **16.000**. El valor predeterminado es **10.000**.

Timeout Interval (Tiempo de espera) Esta opción indica, mediante una "condición de cierre", el tiempo de espera en el que la adición debe finalizar antes de que el temporizador la cierre. El intervalo es de **0** a **100** ms. El valor predeterminado es **10**.

Size of Packet in Aggregation (Tamaño mínimo de paquetes en adición) Esta opción indica el tamaño mínimo (en bytes) de los paquetes acumulados durante la adición. El intervalo es de **0** a **1.500**. El valor predeterminado es **10**.

ADDBA Timeout (Tiempo de espera ADDBA) Esta opción indica el periodo de tiempo tras el que finaliza la configuración ADDBA, si en ese tiempo no se realiza intercambio de tramas según el acuerdo ACK (Confirmación de bloque). El intervalo es de **0** a **65.535** ms. El valor predeterminado es **0**, que desactiva la función de tiempo de espera.

Aggregation Window Size (Tamaño de la ventana de adición) Esta opción indica el número máximo de paquetes que se han transmitido sin confirmación de bloque. El intervalo es de **0** a **64**. El valor predeterminado es **64**.

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Wireless > Advanced Wireless Settings (Inalámbrico > Parámetros inalámbricos avanzados)

Configure las funciones inalámbricas avanzadas del puente. Estos parámetros sólo los debe ajustar un administrador experto, ya que unos parámetros incorrectos pueden reducir el rendimiento inalámbrico.



NOTA
Los parámetros que aparecen en la pantalla *Advanced Wireless Settings* (Parámetros inalámbricos avanzados) están dirigidos a usuarios avanzados.

Advanced Wireless (Parámetros inalámbricos avanzados)

Use LDPC (Utilizar LDPC) LDPC (código de comprobación de paridad de baja densidad) activa o desactiva la corrección de errores para reducir las posibles pérdidas de datos en canales con interferencias. El algoritmo de adaptación de velocidad desactiva de forma automática el código LDPC cuando funciona a velocidades PHY altas (superiores a 162). Para utilizar el esquema de corrección de errores avanzado LDPC, mantenga el valor predeterminado en **Yes** (Sí). De lo contrario, seleccione **No**.

ERP Protection Type (Tipo de protección ERP) Esta opción configura la protección de paquetes OFDM, a pesar de la presencia de estaciones 802.11b dentro de la red inalámbrica. Al enviar paquetes RTS/CTS o CTS2Self a la velocidad de 802.11b, el puente informa a la red inalámbrica de que va a transferir paquetes OFDM. Además, protege los paquetes en la red inalámbrica. Los paquetes RTS/CTS y CTS2Self generan un tiempo de procesamiento, que puede conllevar un rendimiento menor.

La opción RTS/CTS ofrece mejor cobertura, pero menor rendimiento que CTS2Self, ya que incluye confirmación del dispositivo receptor. Para utilizar la opción RTS/CTS, mantenga el valor predeterminado **RTS/CTS**. La opción None (Ninguno) puede provocar colisiones entre los paquetes OFDM y CCK. Para utilizar esta opción, seleccione **None** (Ninguno). Para utilizar la opción CTS2Self, seleccione **CTS2Self**.

11n Protection Type (Tipo de protección 11n) Esta opción configura la protección de los dispositivos que no son de alto rendimiento (HT) dentro de la red inalámbrica. Si el router inalámbrico (o el punto de acceso) detecta una asociación con un dispositivo anterior que no sea de alto rendimiento, indicará a los dispositivos de alto rendimiento que utilicen mecanismos RTS/CTS o CTS2Self antes de cada transmisión de datos. Esta opción también admite toda protección estándar 802.11n, entre otras, MIMO.

La opción RTS/CTS ofrece mejor cobertura, pero menor rendimiento que CTS2Self, ya que incluye confirmación del dispositivo receptor. Para utilizar la opción RTS/CTS, mantenga el valor predeterminado **RTS/CTS**. La opción None (Ninguno) puede provocar colisiones entre los paquetes HT y los anteriores. Para utilizar esta opción, seleccione **None** (Ninguno). Para utilizar la opción CTS2Self, seleccione **CTS2Self**.

Percentage of maximal transmit power (Porcentaje de potencia de transmisión máxima) Esta opción establece el porcentaje de potencia de transmisión máxima relativo a las restricciones de dominio sobre normativas. Por ejemplo, si la restricción de dominio sobre normativas permite transmisiones de hasta 20 dB, cuando se establece el porcentaje al 50% es posible contar con una potencia de transmisión máxima de 10 dB. Seleccione el porcentaje que desea utilizar: **12%**, **25%**, **50%** o **100%**. El valor predeterminado es **100%**.

QoS Classification Type (Tipo de clasificación QoS) Esta opción establece la asignación 802.1D o 802.1Q en el campo IP DSCP/TOS para las prioridades WMM (Fondo, Mayor esfuerzo, Vídeo, Voz). Mantenga el valor predeterminado **802.1D** o seleccione **802.1Q**, que se utiliza en transmisiones IPTV.

Restablezca la conexión Ethernet cuando inicie la conexión inalámbrica Para iniciar la detección DHCP desde el dispositivo que se encuentra detrás del puente, éste restablecerá el enlace Ethernet entre el puente y el dispositivo cada vez que se establezca una conexión inalámbrica. Para desactivar este comportamiento, seleccione **No**. De lo contrario, mantenga el valor predeterminado, **Yes** (Sí).

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Administration > Management (Administración > Gestión)

Utilice esta pantalla para gestionar las funciones específicas del puente: acceso a la utilidad basada en web, copia de seguridad del archivo de configuración y reinicio.



Management (Gestión)

Bridge Access (Acceso al puente)

Utilice una contraseña para proteger el acceso a la utilidad basada en explorador.

Bridge Password (Contraseña del puente) Introduzca una nueva contraseña para el puente.

Re-enter to confirm (Confirmar contraseña) Vuelva a introducir la contraseña para confirmarla.

Idle Timeout (Tiempo de inactividad) El tiempo de inicio de sesión se agota después del tiempo de inactividad que haya especificado. El intervalo es de **60** a **3.600** segundos. El valor predeterminado es **600**.

Acceso web

Access via Wireless (Acceso inalámbrico) Si utiliza el puente en un dominio público donde se concede acceso inalámbrico a los invitados, puede desactivar el acceso inalámbrico a la utilidad basada en explorador del puente. Si desactiva el parámetro sólo podrá acceder a la utilidad basada en explorador mediante una conexión con cable. Mantenga el valor predeterminado, **Enabled** (Activado), para permitir el acceso inalámbrico a la utilidad basada en explorador del puente o bien seleccione **Disabled** (Desactivado) para bloquear el acceso inalámbrico a la utilidad.

Copia de seguridad y restauración

Backup (Copia de seguridad) Para realizar una copia de seguridad del archivo de configuración del puente, haga clic en **Backup Configurations** (Copia de seguridad de la configuración). A continuación, siga las instrucciones que aparecen en pantalla.

Restore (Restaurar) Haga clic en **Browse** (Examinar) y seleccione el archivo de configuración. Por último, haga clic en **Restore Configurations** (Restauración de la configuración).

System Reboot (Reinicio del sistema)

Reboot (Reinicio) Si desea reiniciar el puente, haga clic en **Start to Reboot** (Comenzar reinicio).

Haga clic en **Save Settings** (Guardar parámetros) para guardar los cambios o en **Cancel Changes** (Cancelar cambios) para cancelarlos.

Administration > Factory Defaults (Administración > Parámetros predeterminados de fábrica)

Use esta pantalla para restaurar los parámetros predeterminados de fábrica del puente.

Factory Defaults (Parámetros predeterminados de fábrica)

Restore All Settings (Restaurar todos los parámetros) Si desea restaurar los parámetros predeterminados de fábrica del puente, haga clic en **Restore All Settings** (Restaurar todos los parámetros). Los parámetros que haya guardado se perderán al restaurar los parámetros predeterminados.



Administration > Upgrade Firmware (Administración > Actualizar el firmware)

Utilice esta pantalla para actualizar el firmware del puente. No actualice el firmware a menos que tenga problemas con el puente o desee utilizar una función del nuevo firmware.



Antes de actualizar el firmware, descargue el archivo de actualización del firmware del puente en el sitio web de Linksys, **www.Linksys.com/support**.

Upgrade Firmware (Actualizar el firmware)

Seleccione un archivo para actualizar el firmware Haga clic en **Browse** (Examinar) y seleccione el archivo de actualización del firmware. A continuación, haga clic en **Start to Upgrade** (Iniciar actualización) y siga las instrucciones que aparecen en la pantalla.

Status > Bridge (Estado > Puente)

Se muestra información sobre el estado actual del puente.



Bridge Information (Información del puente)

Firmware Version (Versión del firmware) Muestra el firmware actual del puente.

Local Network (Red local)

Local MAC Address (Dirección MAC local) Muestra la dirección MAC del puente, tal y como se ve en la red Ethernet local.

IP Address (Dirección IP) Muestra la dirección IP del puente, tal y como se ve en la red Ethernet local.

Subnet Mask (Máscara de subred) Muestra la máscara de subred configurada en la red local.

Status > Wireless (Estado > Inalámbrica)

Se muestra información sobre la red inalámbrica.



Wireless (Inalámbrico)

Link Status (Estado de la conexión) Muestra el estado de la conexión de la red inalámbrica.

MAC Address (Dirección MAC) Muestra la dirección MAC del puente, tal y como se ve en la red inalámbrica local.

Network Name (SSID) (Nombre de la red) Muestra el SSID o nombre de la red inalámbrica.

BSSID Muestra la dirección MAC inalámbrica del router inalámbrico o punto de acceso conectado.

Radio Band (Banda de radio) Muestra la banda de radio de la red inalámbrica.

Channel Width (Ancho de canal) Muestra el ancho de canal (en MHz) utilizado por la red inalámbrica.

Wide Channel (Canal ancho) Muestra el canal ancho en función de los parámetros de canal del router de red. Si ha seleccionado el canal ancho de 40 MHz para el parámetro Radio Band (Banda de radio) o Channel Width (Ancho de canal) del router, éste será el canal primario Wireless-N.

Standard Channel (Canal estándar) Muestra el parámetro canal estándar. Si ha seleccionado el canal ancho de 40 MHz para el parámetro Radio Band (Banda de radio) o Channel Width (Ancho de canal) del router, el Canal estándar será un canal secundario para Wireless-N.

Bit Rate (Tasa de bits) Muestra la velocidad de transmisión de datos.

Signal (Señal) Muestra el porcentaje de la potencia de la señal. La potencia máxima de la señal es 100% y la mínima, 0%.

Security (Seguridad) Muestra el método de seguridad de la red inalámbrica.

Resolución de problemas

WES610N/WET610N

El ordenador u otro dispositivo Ethernet con cables no puede establecer comunicación con el router inalámbrico.

1. Abra la utilidad basada en explorador del puente.
2. En la pantalla *Basic Wireless Settings* (Parámetros inalámbricos básicos), asegúrese de que el valor de Network Name (SSID) (Nombre de red [SSID]) coincide con el nombre de su red inalámbrica.
3. Compruebe que los parámetros de seguridad (WPA, WPA2, o WEP) coinciden con los parámetros de seguridad de su red inalámbrica.

Es necesario cambiar la dirección IP del puente.

Si el puente está conectado a una red con un servidor DHCP (normalmente el router de la red), el puente utilizará el servidor DHCP para obtener su dirección IP. Si no hay un servidor DHCP, el puente utilizará la dirección IP estática predeterminada: **169.254.1.250**.

Si desea que el puente utilice siempre la dirección IP estática, siga estas instrucciones:

1. Abra la utilidad basada en explorador del puente.
2. Haga clic en la ficha **Network Setup** (Configuración de red).
3. En el menú desplegable *Network Connection Type* (Tipo de conexión de red), seleccione **Static IP** (IP estática).
4. Rellene los campos *Static IP Address* (Dirección IP estática), *Subnet Mask* (Máscara de subred) y *Default Gateway* (Gateway predeterminada).
5. Haga clic en **Save Settings** (Guardar parámetros).

El equipo u otro dispositivo Ethernet con cables compatible con el puente no establecerá comunicación con otros dispositivos inalámbricos (otro equipo o una impresora).

Compruebe los siguientes puntos:

- Asegúrese de que el dispositivo inalámbrico se encuentra en la misma red inalámbrica que el ordenador u otro dispositivo Ethernet con cables conectado al puente.
- Compruebe que se utiliza el mismo nombre de la red (SSID) para todos los dispositivos de la red inalámbrica.
- Asegúrese de que todos los dispositivos se encuentran en la misma red IP y usan direcciones IP compatibles.

La utilidad basada en explorador no acepta la contraseña.

Compruebe los siguientes puntos:

- La contraseña distingue entre mayúsculas y minúsculas. Asegúrese de que utiliza las mayúsculas y minúsculas correctas al introducir la contraseña.
- Si olvida la contraseña, podrá restablecer el puente a los parámetros predeterminados de fábrica.

 Mantenga pulsado el botón de **reinicio** durante unos cinco segundos para que se restablezca la contraseña predeterminada de fábrica: **admin**. Además, el puente volverá a tener el resto de parámetros predeterminados de fábrica. Para acceder a la utilidad basada en explorador, introduzca **admin** en el campo *Password* (Contraseña).

Después de efectuar cambios mediante la utilidad basada en explorador, los nuevos parámetros no se muestran en la pantalla.

En el explorador web, haga clic en el botón de **actualización**. Si no se muestran los nuevos parámetros, siga estas instrucciones:

1. Desconecte el adaptador de corriente del puente.
2. Espere cinco segundos y vuelva a conectar el adaptador de corriente al puente.
3. En el explorador web, haga clic en el botón de **actualización**.

WEB
Si no ha encontrado respuesta a sus dudas, consulte el sitio web de Linksys en **Linksys.com/support**

Especificaciones

WES610N

Modelo	WES610N
Estándares	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Luz	Alimentación, Ethernet, Wi-Fi Protected Setup™, conexión inalámbrica, actividad y enlace Ethernet individual
Puertos	Ethernet (4), alimentación
Botones	Reinicio, configuración Wi-Fi protegida
Tipo de cableado	CAT 5e
Antenas	3 (internas)
Tipo de conector de antena	N/A
Desmontable (Sí/No)	No
Modulaciones	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Potencia de radiofrecuencia (EIRP) en dBm	802.11a: 15 dBm (habitual) a 54 Mbps 802.11b: 19 dBm (habitual) a 11 Mbps 802.11g: 16 dBm (habitual) a 54 Mbps 802.11n (2,4 GHz): 18 dBm (habitual) a MCS15 802.11n (5 GHz): 16 dBm (habitual) a MCS15
Sensibilidad de recepción	802.11a: -72 dBm (habitual) a 54 Mbps 802.11b: -85 dBm (habitual) a 11 Mbps 802.11g: -73 dBm (habitual) a 54 Mbps 802.11n (20 MHz): -75 dBm (habitual) a MCS15 802.11n (40 MHz): -69 dBm (habitual) a MCS15
Ganancia de la antena en dBi	1
Seguridad inalámbrica	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bits de clave de seguridad	Encriptación de hasta 128 bits

Condiciones ambientales

Dimensiones	177 x 128 x 68 mm (6,97" x 5,04" x 2,68")
Peso	295 g (0,65 libras)
Certificación	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, configuración Wi-Fi protegida, WMM®
Alimentación	12 V, 1 A
Temperatura de funcionamiento	0 a 40 °C (32 a 104 °F)
Temperatura de almacenamiento	-20 a 60 °C (-4 a 140 °F)
Humedad de funcionamiento	Entre el 10% y el 85% sin condensación
Humedad de almacenamiento	Entre el 5% y el 90% sin condensación

Las especificaciones pueden cambiar sin previo aviso.

WET610N

Modelo	WET610N
Estándares	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Luces	Alimentación, Ethernet, Wi-Fi Protected Setup™, conexión inalámbrica
Puertos	Ethernet, alimentación
Botones	Reinicio, configuración Wi-Fi protegida
Tipo de cableado	CAT 5e
Antenas	3 (internas)
Tipo de conector de antena	N/A
Desmontable (Sí/No)	No
Modulaciones	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Potencia de radiofrecuencia (EIRP) en dBm	802.11a: 15 dBm (habitual) a 54 Mbps 802.11b: 18 dBm (habitual) a 11 Mbps 802.11g: 16 dBm (habitual) a 54 Mbps 802.11n: 12 dBm (habitual) a 130 Mbps (HT20), 270 Mbps (HT40)
Sensibilidad de recepción	802.11a: -72 dBm (habitual) a 54 Mbps 802.11b: -85 dBm (habitual) a 11 Mbps 802.11g: -73 dBm (habitual) a 54 Mbps 802.11n: -70 dBm (habitual) a MCS15/2,4 GHz, -69 dBm (habitual) a MCS15/5,0 GHz
Ganancia de la antena en dBi	1
Seguridad inalámbrica	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bits de clave de seguridad	Encriptación de hasta 128 bits

Condiciones ambientales

Dimensiones	145 x 106 x 52 mm (5,71" x 4,17" x 2,05")
Peso	159 g (5,61 onzas)
Certificación	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, configuración Wi-Fi protegida, WMM®
Alimentación	12 V, 1 A
Temperatura de funcionamiento	0 a 40 °C (32 a 104 °F)
Temperatura de almacenamiento	-20 a 60 °C (-4 a 140 °F)
Humedad de funcionamiento	Entre el 10% y el 85% sin condensación
Humedad de almacenamiento	Entre el 5% y el 90% sin condensación

Las especificaciones pueden cambiar sin previo aviso.

Linksys.com/support

Cisco, el logotipo de Cisco y Linksys son marcas comerciales o marcas registradas de Cisco y/o sus filiales en EE. UU. y otros países.
Puede encontrar una lista con las marcas comerciales de Cisco en www.cisco.com/go/trademarks. Todas las demás marcas comerciales mencionadas en este documento son propiedad de sus respectivos dueños.

© 2011 Cisco y/o sus filiales. Todos los derechos reservados.

3425-01249



Käyttöopas

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Sisällys

Tuotteen yleiskatsaus

Merkkivalot 2
Portit 3

Langattoman verkon suojauksen tarkistusluettelo

Muuta langattoman verkon oletusnimeä eli SSID-tunnusta 4
Muuta oletussalasanaa 4
Ota MAC-osoitteiden suodatus käyttöön 4
Ota salaus käyttöön 4
Yleisiä ohjeita verkon suojaamiseen 4
Lisävihjeitä suojaamiseen 5

Lisämääritykset

Selainapuohjelman avaaminen 6
Setup (Asetukset) > Basic Setup (Perusasetukset) 7
Language (Kieli) 7
Network Setup (Verkkoasetukset) 7
Wireless (Langaton verkko) > Basic Wireless Settings (Langattoman verkon perusasetukset) 7
Basic Wireless Settings (Langattoman verkon perusasetukset) 8
Wireless Security (Langattoman verkon suojaus) 8
Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys) 9
Wireless (Langaton verkko) > Wireless Network Site Survey (Langattoman verkon etsintä) 10
Wireless Network Site Survey (Langattoman verkon etsintä) 10
Wireless (Langaton verkko) > WMM® 11
WMM 12
Wireless (Langaton verkko) > Advanced Wireless Settings (Langattoman verkon lisäasetukset) 13
Advanced Wireless (Langattoman verkon lisäasetukset) 14
Administration (Valvonta) > Management (Hallinta) 14
Management (Hallinta) 15
Administration (Valvonta) > Factory Defaults (Tehdasoletukset) 15
Factory Defaults (Tehdasoletukset) 15
Administration (Valvonta) > Upgrade Firmware (Laiteohjelmiston päivitys) 15
Upgrade Firmware (Laiteohjelmiston päivitys) 15
Status (Tila) > Bridge (Silta) 16
Bridge Information (Sillan tiedot) 16
Local Network (Lähiverkko) 16
Status (Tila) > Wireless (Langaton verkko) 16
Wireless (Langaton verkko) 16

Vianmääritys

WES610N/WET610N 17

Tekniset tiedot

WES610N 18
WET610N 19

Tuotteen yleiskatsaus

Kiitos, että olet valinnut Linksys Dual-Band N Entertainment Bridge -sillan. Sillan avulla voit yhdistää minkä tahansa johdollisen Ethernet-laitteen langattomaan verkkoosi. Silta perustuu dual-band Wireless-N -tekniikkaan, joten se on yhteensopiva minkä tahansa Wireless-N, -G, -A tai -B-reitittimen tai tukiaseman kanssa. Kun asennat sillan ensimmäistä kertaa, seuraa CD-kansiossa olevia ohjeita. Määritä lisäasetukset kätevän selainpohjaisen apuohjelman avulla.

Merkkivalot



WES610N WET610N

Langaton yhteys (sininen) Langattoman yhteyden merkkivalo palaa, kun langaton yhteys on käytössä. Merkkivalo vilkkuu, kun silta lähettää tai vastaanottaa tietoja aktiivisesti langattoman verkon kautta.

Wi-Fi Protected Setup -painike Jos reititin tukee Wi-Fi Protected Setup -toimintoa ja käyttää WPA- tai WPA2-suojausta, voit muodostaa siltaan yhteyden automaattisesti Wi-Fi Protected Setup -toiminnon avulla. Lisätietoja Wi-Fi Protected Setup -toiminnon käytöstä on kohdassa "Wireless (Langaton verkko) > Basic Wireless Settings (Langattoman verkon perusasetukset)" sivulla 7.

Wi-Fi Protected Setup -merkkivalo (sininen/keltainen) Merkkivalo vilkkuu sinisenä kaksi minuuttia Wi-Fi Protected Setup -toiminnan aikana. Kun langattoman yhteyden suojaus on käytössä, valo palaa sinisenä. Jos Wi-Fi Protected Setup -prosessin aikana tapahtuu virhe, merkkivalo palaa keltaisena. Tarkista, että verkkoreititin tukee Wi-Fi Protected Setup -toimintoa. Odota, kunnes merkkivalo on sammunut, ja yritä sitten uudelleen.

Ethernet (sininen) Ethernet-merkkivalo palaa, kun kiinteä yhteys on käytössä. Merkkivalo vilkkuu, kun silta lähettää tai vastaanottaa tietoja aktiivisesti Ethernet-porttien kautta.

Virta (sininen) Virran merkkivalo palaa, kun silta on päällä.

Portit



WES610N WET610N

Ethernet Silta yhdistetään tietokoneeseen tai muuhun Ethernet-laitteeseen Ethernet portin/porttien kautta. WES610N-mallissa on neljä porttia, WET610N-mallissa yksi.

Reset Sillan tehdasasetukset voi palauttaa kahdella eri tavalla: pitämällä Reset-painiketta painettuna noin viiden sekunnin ajan tai palauttamalla oletusasetukset sillan selainpohjaisen apuohjelman kautta valitsemalla Administration (Valvonta) > Factory Defaults (Tehdasoletukset). WES610N-mallin Reset-painike on laitteen pohjassa, WET610N-mallin Reset-painike laitteen takapaneelissa.

Virta Virtaporttiin kytketään sillan virtasovitin.

Langattoman verkon suojauksen tarkistusluettelo

Langattomat verkot ovat käteviä ja helppoja asentaa, ja niinpä ne yleistyvätkin nopeasti kodeissa, joissa on laajakaistainen Internet-yhteys. Langaton verkko toimii radioaaltojen avulla, ja siksi se on alttiimpi luvattomalle käytölle kuin perinteinen langallinen verkko. Matkapuhelimien ja langattomien puhelimien signaalien tapaan myös langattoman verkon signaaleja voidaan käyttää luvattomasti. Ulkopuolisia ei voi fyysisesti estää käyttämästä langatonta verkkoa, joten verkko on suojattava lisäasetuksilla.

Muuta langattoman verkon oletusnimeä eli SSID-tunnusta

Langattoman verkon laitteilla on tehtaassa asetettu oletusverkkonimi, eli SSID-tunnus (Service Set Identifier). Se on langattoman verkon nimi, ja sen enimmäispituus on 32 merkkiä. Langattomat Linksys-tuotteet käyttävät langattoman verkon oletusnimenä nimeä **linksys**. Muuta langattoman verkon nimeä niin, että erotat sen helposti mahdollisista muista lähistöllä toimivista langattomista verkoista. Älä kuitenkaan käytä nimessä mitään henkilökohtaisia tietoja (kuten henkilötunnustasi), koska verkon nimi näkyy kaikille, jotka lähistöllä selaavat langattomien verkkojen nimiä.

Muuta oletussalasanaa

Tukiasemat, reitittimet ja muut langattoman verkon laitteet kysyvät salasanaa, jos niiden asetuksia yritetään muuttaa. Näissä laitteissa on tehtaassa asetettu oletussalasana. Linksys-laitteiden oletussalasana on **admin**. Ulkopuoliset voivat tietää nämä oletusasetukset ja yrittää tunkeutua niiden avulla langattomaan laitteeseen ja muuttaa verkkoasetuksia. Voit estää luvattomat muutokset muuttamalla laitteen salasanan vaikeasti arvattavaksi.

Ota MAC-osoitteiden suodatus käyttöön

Linksys-reitittimissä voi ottaa käyttöön MAC (Media Access Control) -osoitteiden suodatuksen. MAC-osoite on yksilöivä numero- ja kirjainsarja, joka määritetään verkon jokaiselle laitteelle. Kun MAC-osoitteiden suodatus on käytössä, langatonta verkkoa voivat käyttää vain ne langattomat laitteet, joilla on tietty MAC-osoite. Voit esimerkiksi määrittää kotisi jokaisen tietokoneen MAC-osoitteen niin, että vain kyseiset tietokoneet voivat käyttää langatonta verkkoa.

Ota salaus käyttöön

Salaus suojaa langattomassa verkossa siirrettäviä tietoja. WPA- tai WPA2-salaus (Wi-Fi Protected Access) ja WEP-salaus (Wired Equivalent Privacy) mahdollistavat vahvuudeltaan erilaisten suojausten käyttämisen langattomassa tiedonsiirrossa.

WPA- tai WPA2-salauksella suojattu verkko on turvallisempi kuin WEP-salauksella suojattu verkko, koska WPA ja WPA2 käyttävät dynaamisia salausavaimia. Radioaalloilla siirrettävien tietojen suojaamiseksi verkkolaitteissa kannattaa käyttää vahvinta mahdollista salausta.

WEP on vanha salausstandardi, joka voi olla ainoa vaihtoehto vanhoissa laitteissa, jotka eivät tue WPA-salausta.

Yleisiä ohjeita verkon suojaamiseen

Langattoman verkon suojauksesta ei ole hyötyä, jos sen perustana oleva verkko ei ole turvallinen.

- Suojaa verkon kaikki tietokoneet salasanalla ja suojaa arkaluontoiset tiedostot erikseen salasanalla.
- Muuta salasanoja säännöllisesti.
- Asenna virustorjunta- ja palomuuriohjelmisto.
- Poista tiedostojen jakaminen (vertaisverkkokäyttö) käytöstä Jotkin sovellukset voivat avata tiedostojen jakamisen pyytämättä vahvistustasi ja/tai tietämättäsi.

Lisävihjeitä suojaamiseen

- Pidä langattomat reitittimet, tukiasemat ja yhdyskäytävät etäällä ulkoseinistä ja ikkunoista.
- Katkaise langattomista reitittimistä, tukiasemista ja yhdyskäytävistä virta, jos niitä ei ole tarkoitus käyttää (esimerkiksi yön tai lomamatkan ajaksi).
- Käytä vahvoja salauslauseita, jotka ovat vähintään kahdeksan merkin pituisia. Käytä sekä kirjaimia että numeroita, äläkä käytä normaaleja kielen sanoja.

Lisämääritykset

Kun silta on määritetty CD-kansion ohjeiden mukaisesti, se on käyttövalmis. Jos haluat muuttaa lisäasetuksia, käytä sillan selainapuohjelmaa. Tässä luvussa on kuvattu apuohjelman kunkin web-sivun sisältö ja kunkin sivun tärkeimmät toiminnot. Apuohjelmaa voi käyttää web-selaimella tietokoneessa, joka on kytketty siltaan.

Selainapuohjelman päävälilehdet: Setup (Asetukset), Wireless (Langaton verkko), Administration (Valvonta) ja Status (Tila). Kun jokin päävälilehdistä valitaan, näkyviin tulee muita välilehtiä.

Selainapuohjelman avaaminen

Selainapuohjelmaa käytetään verkkoselaimen kautta.

Jos silta on liitetty verkkoon, jossa on DHCP-palvelin (yleensä verkkoreititin), silta saa IP-osoitteensa DHCP-palvelimelta. Jos verkossa ei ole DHCP-palvelinta, silta käyttää staattista oletus-IP-osoitetta **169.254.1.250**. (Jos määrität sillalle pysyvän staattisen IP-osoitteen selainapuhojelman kautta, anna staattinen IP-osoite.)

HUOMAUTUS
Jos et tiedä sillan IP-osoitetta, etsi se reitittimen DHCP-asiakastaulukosta. (Lisätietoja on reitittimen käyttöoppaassa.)

Jos et löydä sillan IP-osoitetta, voit palauttaa sillan tehdasasetukset painamalla **Reset**-painiketta noin viiden sekunnin ajan suoristetulla paperiliittimellä. Tämä palauttaa sillan tehdasasetukset. Silta pyytää IP-osoitteen DHCP-palvelimelta (yleensä verkkoreititin). Jos DHCP-palvelinta ei löydy, silta käyttää staattista oletus-IP-osoitetta (**169.254.1.250**), kunnes se löytää DHCP-palvelimen ja saa dynaamisen IP-osoitteen.

Jos siltaan ei ole kytketty reititintä ja se käyttää tehdasasetuksia, pääset selainapuohjelmaan kytkemällä siltaan tietokoneen Ethernet-yhteydellä. Tietokoneen Ethernet-yhteyden staattinen IP-osoite ja aliverkon peite täytyy tällöin määrittää.

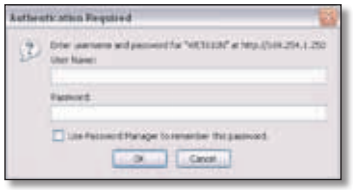
Ethernet-sovittimen IP-osoitteeksi pitää määrittää tietty osoite.

1. Kirjoita *IP address* (IP-osoite) -kenttään **169.254.x.y** (x korvataan numerolla 1–254 ja y numerolla 0–255).
2. Kirjoita *Subnet mask* (Aliverkon peite) -kenttään **255.255.0.0**.

HUOMAUTUS
Staattisen IP-osoitteen määrittäminen tietokoneen Ethernet-sovittimelle tapahtuu eri lailla käyttöjärjestelmästä riippuen. Lisäohjeita saat oman käyttöjärjestelmäsi käyttöoppaasta.

Kun olet määrittänyt Ethernet-sovittimelle staattisen IP-osoitteen, käynnistä internet-selain ja kirjoita sovittimen IP-osoite (oletuksena on **169.254.1.250**) *selaimen osoiteriville*. Paina **Enter**-näppäintä.

Näyttöön tulee salasanaikkuna. (Esimerkki Windows XP:stä. Muissa käyttöjärjestelmissä näyttöön tulee samantapainen ikkuna.) Jätä *User name* (Käyttäjätunnus) -kenttä tyhjäksi. Anna ohjatun asennuksen yhteydessä luomasi salasana. Jos et luonut uutta salasanaa, kirjoita kenttään oletussalasana **admin**. (Voit asettaa uuden salasanan kohdassa *Administration* (Valvonta) > *Management* (Hallinta).) Jatka valitsemalla **OK**.



HUOMAUTUS
Jos salasanaikkuna ei ilmesty näyttöön, odota kaksi minuuttia ja yritä uudelleen.

Setup (Asetukset) > Basic Setup (Perusasetukset)

Ensimmäisenä tulee näkyviin *Basic Setup* (Perusasetukset) -näyttö. Tässä näytössä voit muuttaa selainapuohjelman kieltä tai sillan kiinteän Ethernet-verkon asetuksia.





Language (Kieli)

Language (Kieli) Voit muuttaa selainapuohjelman kieltä. Valitse haluamasi kieli avattavasta valikosta.

Network Setup (Verkkoasetukset)

Voit määrittää, hakeeko silta IP-osoitteen automaattisesti DHCP-palvelimelta, kuten verkkoreitittimeltä (Automatic Configuration (Automaattinen määritys) - DHCP), vai asetetaanko se manuaalisesti (Static IP (Staattinen IP)).

Bridge IP (Sillan IP) Jos verkossasi on DHCP-palvelin (kuten verkkoreititin), joka määrittää IP-osoitteita verkkolaitteille, pidä oletusasetus **Automatic Configuration - DHCP** (Automaattinen määritys - DHCP). Silta pyytää IP-osoitteen DHCP-palvelimelta (yleensä verkkoreititin). Jos DHCP-palvelinta ei löydy, silta käyttää staattista oletus-IP-osoitetta (**169.254.1.250**), kunnes se löytää DHCP-palvelimen ja saa dynaamisen IP-osoitteen.

Jos haluat määrittää sillalle pysyvän staattisen IP-osoitteen, valitse **Static IP** (Staattinen IP).

Jos valitset asetukseksi Static IP (Staattinen IP), täytä seuraavat kentät:

- **Static IP Address** (Staattinen IP-osoite) Anna yksilöivä IP-osoite, jonka avulla voidaan luoda yhteys selainapuohjelmaan.
- **Subnet Mask** (Aliverkon peite) Anna kiinteän verkon aliverkon peite.
- **Default Gateway** (Oletusyhdyskäytävä) Anna verkon oletusyhdyskäytävän IP-osoite (useimmiten reititin).

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Wireless (Langaton verkko) > Basic Wireless Settings (Langattoman verkon perusasetukset)

Määritä sillan langattoman verkon perusasetukset ja suojausasetukset *Basic Wireless Settings* (Langattoman verkon perusasetukset) -näytössä.

Sillan asetukset voi määrittää kahdella tavalla: manuaalisesti tai Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys) -toiminnon avulla. Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys) -toiminnon avulla langattoman verkon asetusten määrittäminen on helppoa. Jos verkkoreitittimesi tukee Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys) -toimintoa ja käyttää WPA- tai WPA2-suojausta, voit muodostaa siltaan automaattisesti yhteyden Wi-Fi Protected Setup -toiminnolla.

Configuration View (Määritysnäkymä) Jos haluat määrittää langattoman verkon asetukset itse, valitse **Manual** (Manuaalinen). Lisätietoja kohdassa **Basic Wireless Settings** (Langattoman verkon perusasetukset), **sivu 8**. Jos haluat käyttää Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys) -toimintoa, valitse **Wi-Fi Protected Setup** (Wi-Fi-asetusten automaattinen määritys). Lisätietoja kohdassa **Wi-Fi Protected Setup** (Wi-Fi-asetusten automaattinen määritys), **sivu 9**.

Basic Wireless Settings (Langattoman verkon perusasetukset)



Network Name (SSID) (Verkon nimi (SSID)) SSID on verkon nimi, jonka kaikki langattoman verkon laitteen jakavat. Kaikilla saman langattoman verkon laitteilla on oltava sama SSID. Isoilla ja pienillä kirjaimilla on eri merkitys, ja nimen enimmäispituus on 32 merkkiä (kaikki näppäimistön merkit kelpaavat). Varmista, että asetus vastaa langattoman reitittimen tai yhteyspisteen asetusta. Jos haluat parantaa suojausta, muuta SSID-nimen oletusasetus (**linksys**) muuksi yksilöiväksi nimeksi.

Wireless Security (Langattoman verkon suojaus)

Silta tukee seuraavia langattoman verkon suojausvaihtoehtoja: WPA Personal, WPA2 Personal ja WEP. WPA (Wi-Fi Protected Access) ja WPA2 ovat tehokkaampia suojaustapoja kuin WEP (Wired Equivalent Privacy). Lisätietoja langattoman verkon suojaamisesta on kohdassa "Langattoman verkon suojauksen tarkistusluettelo", sivu 4.

Security Mode (Suojaustila)

Valitse suojaustila langatonta verkkoa varten. Jos et halua suojata langatonta verkkoa, pidä oletusasetus **Disabled** (Ei käytössä).

HUOMAUTUS
Jokaisen langattomassa verkossa olevan laitteen pitää käyttää samaa suojausta ja salasanaa/suojausavainta, tai laitteet eivät pysty kommunikoimaan keskenään.

WPA Personal

WPA on vahvempi suojausstandardi kuin WEP-salaus.



Encryption (Salaus) WPA tukee TKIP-salausta, joka käyttää dynaamisia salausavaimia.

Passphrase (Salasana) Anna sillan ja langattoman reitittimen tai yhteyspisteen käytössä oleva tunnus. Sen pitää koostua 8-63 merkistä.

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

WPA2 Personal

WPA2 on kehittyneempi ja tehokkaampi versio WPA:sta.



Encryption (Salaus) WPA2 tukee kahta salausmenetelmää: TKIP ja AES. Niissä käytetään dynaamisia salausavaimia. Valitse salausmenetelmä: **AES**, **TKIP tai AES**. Oletusasetus on **AES**.

Passphrase (Salasana) Anna sillan ja langattoman reitittimen tai yhteyspisteen käytössä oleva tunnus. Sen pitää koostua 8-63 merkistä.

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

WEP

WEP on perussalausmenetelmä, joka ei ole yhtä turvallinen kuin WPA tai WPA2.



Encryption (Salaus) Valitse WEP-salauksen taso vaihtoehdoista **40/64 bits (10 hex digits)** (40/64 bittiä (10 heksadesimaalilukua)) tai **104/128 bits (26 hex digits)** (104/128 bittiä (26 heksadesimaalilukua)). Oletus on **40/64 bits (10 hex digits)** (40/64 bittiä (10 heksadesimaalilukua)).

Key 1 (Avain 1) Anna verkon WEP-avain.

Tx Key (Tx-avain) **Key 1** (Avain 1) on sillan käyttämä lähetysavain.

Authentication (Todennus) Oletuksena on **Auto** (Automaattinen), ja se mahdollistaa avoimen järjestelmän käytön tai todennuksen jaetun avaimen avulla. Valitse **Open** (Avoin), jos haluat käyttää avointa järjestelmää, jossa lähettäjä ja vastaanottaja eivät käytä WEP-avainta todennukseen. Valitse **Shared** (Jaettu), jos haluat käyttää todennusta jaetun avaimen avulla, jossa lähettäjä ja vastaanottaja käyttävät WEP-avainta todennukseen.

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys)

Valittavissa on kaksi menetelmää. Valitse menetelmä käytössä olevan reitittimen mukaan.





Menetelmä 1

Käytä tätä menetelmää, jos reitittimessä on Wi-Fi Protected Setup -painike.

1. Napsauta tai paina reitittimen **Wi-Fi Protected Setup** -painiketta.
2. Napsauta **Wi-Fi Protected Setup** -painiketta sillan *Wi-Fi Protected Setup* (Wi-Fi-asetusten automaattinen määritys) -näytössä.
3. Kun silta on määritetty, valitse **Close** (Sulje).

Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys) -näytössä näkyy Link Status (Yhteyden tila), Network Name (SSID) (Verkkonimi (SSID) ja Security method (Suojausmenetelmä).

Menetelmä 2

Käytä tätä menetelmää, jos reititin pyytää sillan PIN-tunnusta.

1. Kirjoita **reitittimen** *Wi-Fi Protected Setup* (Wi-Fi-asetusten automaattinen määritys) -näyttöön **sillan** *Wi-Fi Protected Setup* (Wi-Fi-asetusten automaattinen määritys) -näytössä oleva PIN-tunnus. Valitse sitten **Register** (Rekisteröi) tai vastaava painike. (Se on merkitty myös sillan pohjaan.)
2. Valitse **OK sillan** *Wi-Fi Protected Setup* (Wi-Fi-asetusten automaattinen määritys) -näytössä.
3. Kun silta on määritetty, valitse **Close** (Sulje).

Wi-Fi Protected Setup (Wi-Fi-asetusten automaattinen määritys) -näytössä näkyy Link Status (Yhteyden tila), Network Name (SSID) (Verkkonimi (SSID) ja Security method (Suojausmenetelmä).

Wireless (Langaton verkko) > Wireless Network Site Survey (Langattoman verkon etsintä)

Aloita langattoman verkon etsintä avaamalla **Wireless Network Site Survey** (Langattoman verkon etsintä) -välilehti. *Wireless Network Site Survey* (Langattoman verkon etsintä) -näytöllä näkyvät sillan havaitsemat langattomat verkot.



Wireless Network Site Survey (Langattoman verkon etsintä)

Number of Wireless Networks (Langattomien verkkojen määrä) Sillan havaitsemien langattomien verkkojen määrä.

Select (Valitse) Muodosta yhteys langattomaan verkkoon valitsemalla **Select** (Valitse). Napsauta sitten **Connect** (Yhdistä).

Wireless Network Name (Langattoman verkon nimi) Langattoman verkon verkkonimi eli SSID.

GHz Langattoman verkon radiotaajuus.

Signal (Signaali) Signaalin voimakkuus prosentteina. 100 % on vahvin mahdollinen signaali, 0 % heikoin.

Security (Suojaus) Jos verkko tukee Wi-Fi Protected Setup -toimintoa sen kuvake on näkyvissä. Langattoman verkon käyttämä suojausmenetelmä on näkyvissä.

Päivitä näytöllä näkyvät tiedot valitsemalla **Refresh** (Päivitä).

Kun volet valinnut verkon, valitse **Connect** (Yhdistä). Uusi näyttö tulee näkyviin. Noudata verkon suojausmenetelmän ohjeita.

WPA



Network Name (SSID) (Verkkonimi (SSID)) Valitsemasi verkon nimi näkyy automaattisesti.

Security Mode (Suojaustila) WPA Personal näkyy automaattisesti.

Encryption (Salaus) WPA tukee TKIP-salausta, joka käyttää dynaamisia salausavaimia.

Passphrase (Salasana) Anna sillan ja langattoman reitittimen tai yhteyspisteen käytössä oleva tunnus. Sen pitää koostua 8-63 merkistä.

Päivitä näytöllä näkyvät tiedot valitsemalla **Refresh** (Päivitä).

Kun olet antanut suojausasetukset, valitse **Connect** (Yhdistä).

WPA2



Network Name (SSID) (Verkkonimi (SSID)) Valitsemasi verkon nimi näkyy automaattisesti.

Security Mode (Suojaustila) WPA2 Personal näkyy automaattisesti.

Encryption (Salaus) WPA2 tukee kahta salausmenetelmää: TKIP ja AES. Niissä käytetään dynaamisia salausavaimia. Valitse salausmenetelmä: **AES**, **TKIP tai AES**.

Passphrase (Salasana) Anna sillan ja langattoman reitittimen tai yhteyspisteen käytössä oleva tunnus. Sen pitää koostua 8-63 merkistä.

Päivitä näytöllä näkyvät tiedot valitsemalla **Refresh** (Päivitä).

Kun olet antanut suojausasetukset, valitse **Connect** (Yhdistä).

WEP



Network Name (SSID) (Verkkonimi (SSID)) Valitsemasi verkon nimi näkyy automaattisesti.

Security Mode (Suojaustila) WEP näkyy automaattisesti.

Encryption (Salaus) Valitse WEP-salauksen taso vaihtoehdoista **40/64 bits (10 hex digits)** (40/64 bittiä (10 heksadesimaalilukua)) ja **104/128 bits (26 hex digits)** (104/128 bittiä (26 heksadesimaalilukua)).

Key 1 (Avain 1) Anna verkon WEP-avain.

Tx Key (Tx-avain) **Key 1** (Avain 1) on sillan käyttämä lähetysavain.

Authentication (Todennus) Oletuksena on **Auto** (Automaattinen), ja se mahdollistaa avoimen järjestelmän käytön tai todennuksen jaetun avaimen avulla. Valitse **Open** (Avoin), jos haluat käyttää avointa järjestelmää, jossa lähettäjä ja vastaanottaja eivät käytä WEP-avainta todennukseen. Valitse **Shared** (Jaettu), jos haluat käyttää todennusta jaetun avaimen avulla, jossa lähettäjä ja vastaanottaja käyttävät WEP-avainta todennukseen.

Päivitä näytöllä näkyvät tiedot valitsemalla **Refresh** (Päivitä).

Kun olet antanut suojausasetukset, valitse **Connect** (Yhdistä).

Wireless (Langaton verkko) > WMM®

Määritä langattoman multimedian (WMM) asetukset. WMM priorisoi paketteja niiden toiminta-/liikennetyyppien perusteella: Background (Tausta), Best Effort (paras yritys), Video (Video) tai Voice (Ääni). Vain asiantuntevan järjestelmänvalvojan tulisi muuttaa näitä asetuksia, sillä väärät asetukset voivat heikentää langattoman verkon toimivuutta.



HUOMAUTUS
WMM-näytön asetukset on tarkoitettu vain edistyneille käyttäjille.

WMM

Access Mode (Vuorovaikutustyyppi)

Voit määrittää neljälle vuorovaikutustyypille eri asetuksia. Valitse tila, jonka haluat määrittää: **Background** (Tausta), **Best Effort** (Paras yritys), **Video** (Video) tai **Voice** (Ääni). Seuraa valitsemasi tilan ohjeita.

Background (Tausta)

Use Aggregation (Käytä aggregointia) Määrittää, luoko MAC (Media Access Control) -kerros ADDBA (Add Block Acknowledgement) -istunnon. Oletus on **No** (Ei). Valitse **Yes** (Kyllä), jos haluat ottaa toiminnon käyttöön.

Accept Aggregation (Hyväksy aggregointi) Määrittää, hyväksyykö MAC-kerros ADDBA-pyynnön. Oletuksena on **Yes** (Kyllä). Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei).

Max. Number of Packets in Aggregation (Pakettien enimmäismäärä aggregoinnissa) Määrittää pakettien (alikehysten) enimmäismäärän aggregoinnissa. Arvo voi olla välillä **0** - **7**. Oletus on **7**.

Max. Aggregation Size (Aggregoinnin enimmäiskoko) Määrittää aggregoinnin enimmäiskoon bitteinä. Arvo voi olla välillä **0** - **16000**. Oletus on **12000**.

Timeout Internal (Sisäinen aikakatkaisu) Määrittää aikavälin, jolloin aggregointi pitäisi sulkea "sulkemisehdolla", ennen kuin ajastin sulkee sen. Arvo voi olla välillä **0** - **100** ms. Oletus on **3**.

Min. Size of Packet in Aggregation (Paketin vähimmäiskoko aggregoinnissa) Määrittää aggregoinnissa kerättävän paketin vähimmäiskoon bitteinä. Arvo voi olla välillä **0** - **1500**. Oletus on **10**.

ADDBA Timeout (ADDBA-aikakatkaisu) Määrittää keston, jonka jälkeen ADDBA katkaistaan, jos yhtään kehystä ei ole lähetetty tai vastaanotettu Block ACK -sopimuksen alaisena. Arvo voi olla välillä **0** - **65535** ms. Oletus on **0**, mikä poistaa aikakatkaisun käytöstä.

Aggregation Window Size (Aggregoinnin ikkunakoko) Määrittää ilman ACK-kuittauksia siirrettävien pakettien enimmäismäärän. Arvo voi olla välillä **0** - **64**. Oletus on **64**.

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Best Effort (Paras yritys)

Use Aggregation (Käytä aggregointia) Määrittää, luoko MAC (Media Access Control) -kerros ADDBA (Add Block Acknowledgement) -istunnon. Oletuksena on **Yes** (Kyllä). Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei).

Accept Aggregation (Hyväksy aggregointi) Määrittää, hyväksyykö MAC-kerros ADDBA-pyynnön. Oletuksena on **Yes** (Kyllä). Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei).

Max. Number of Packets in Aggregation (Pakettien enimmäismäärä aggregoinnissa) Määrittää pakettien (alikehysten) enimmäismäärän aggregoinnissa. Arvo voi olla välillä **0** - **10**. Oletus on **10**.

Max. Aggregation Size (Aggregoinnin enimmäiskoko) Määrittää aggregoinnin enimmäiskoon bitteinä. Arvo voi olla välillä **0** - **20000**. Oletus on **16000**.

Timeout Internal (Sisäinen aikakatkaisu) Määrittää aikavälin, jolloin aggregointi pitäisi sulkea "sulkemisehdolla", ennen kuin ajastin sulkee sen. Arvo voi olla välillä **0** - **100** ms. Oletus on **3**.

Min. Size of Packet in Aggregation (Paketin vähimmäiskoko aggregoinnissa) Määrittää aggregoinnissa kerättävän paketin vähimmäiskoon bitteinä. Arvo voi olla välillä **0** - **1500**. Oletus on **10**.

ADDBA Timeout (ADDBA-aikakatkaisu) Määrittää keston, jonka jälkeen ADDBA katkaistaan, jos yhtään kehystä ei ole lähetetty tai vastaanotettu Block ACK -sopimuksen alaisena. Arvo voi olla välillä **0** - **65535** ms. Oletus on **0**, mikä poistaa aikakatkaisun käytöstä.

Aggregation Window Size (Aggregoinnin ikkunakoko) Määrittää ilman ACK-kuittauksia siirrettävien pakettien enimmäismäärän. Arvo voi olla välillä **0** - **64**. Oletus on **64**.

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Video

Use Aggregation (Käytä aggregointia) Määrittää, luoko MAC (Media Access Control) -kerros ADDBA (Add Block Acknowledgement) -istunnon. Oletuksena on **Yes** (Kyllä). Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei).

Accept Aggregation (Hyväksy aggregointi) Määrittää, hyväksyykö MAC-kerros ADDBA-pyynnön. Oletuksena on **Yes** (Kyllä). Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei).

Max. Number of Packets in Aggregation (Pakettien enimmäismäärä aggregoinnissa) Määrittää pakettien (alikehysten) enimmäismäärän aggregoinnissa. Arvo voi olla välillä **0** - **7**. Oletus on **7**.

Max. Aggregation Size (Aggregoinnin enimmäiskoko) Määrittää aggregoinnin enimmäiskoon bitteinä. Arvo voi olla välillä **0** - **16000**. Oletus on **12000**.

Timeout Internal (Sisäinen aikakatkaisu) Määrittää aikavälin, jolloin aggregointi pitäisi sulkea "sulkemisehdolla", ennen kuin ajastin sulkee sen. Arvo voi olla välillä **0** - **100** ms. Oletus on **3**.

Min. Size of Packet in Aggregation (Paketin vähimmäiskoko aggregoinnissa) Määrittää aggregoinnissa kerättävän paketin vähimmäiskoon bitteinä. Arvo voi olla välillä **0** - **1500**. Oletus on **10**.

ADDBA Timeout (ADDBA-aikakatkaisu) Määrittää keston, jonka jälkeen ADDBA katkaistaan, jos yhtään kehystä ei ole lähetetty tai vastaanotettu Block ACK -sopimuksen alaisena. Arvo voi olla välillä **0** - **65535** ms. Oletus on **0**, mikä poistaa aikakatkaisun käytöstä.

Aggregation Window Size (Aggregoinnin ikkunakoko) Määrittää ilman ACK-kuittauksia siirrettävien pakettien enimmäismäärän. Arvo voi olla välillä **0** - **64**. Oletus on **64**.

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Voice (Ääni)

Use Aggregation (Käytä aggregointia) Määrittää, luoko MAC (Media Access Control) -kerros ADDBA (Add Block Acknowledgement) -istunnon. Oletuksena on **Yes** (Kyllä). Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei).

Accept Aggregation (Hyväksy aggregointi) Määrittää, hyväksyykö MAC-kerros ADDBA-pyynnön. Oletuksena on **Yes** (Kyllä). Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei).

Max. Number of Packets in Aggregation (Pakettien enimmäismäärä aggregoinnissa) Määrittää pakettien (alikehysten) enimmäismäärän aggregoinnissa. Arvo voi olla välillä **0** - **2**. Oletus on **2**.

Max. Aggregation Size (Aggregoinnin enimmäiskoko) Määrittää aggregoinnin enimmäiskoon bitteinä. Arvo voi olla välillä **0** - **16000**. Oletus on **10000**.

Timeout Internal (Sisäinen aikakatkaisu) Määrittää aikavälin, jolloin aggregointi pitäisi sulkea "sulkemisehdolla", ennen kuin ajastin sulkee sen. Arvo voi olla välillä **0** - **100** ms. Oletus on **10**.

Min. Size of Packet in Aggregation (Paketin vähimmäiskoko aggregoinnissa) Määrittää aggregoinnissa kerättävän paketin vähimmäiskoon bitteinä. Arvo voi olla välillä **0** - **1500**. Oletus on **10**.

ADDBA Timeout (ADDBA-aikakatkaisu) Määrittää keston, jonka jälkeen ADDBA katkaistaan, jos yhtään kehystä ei ole lähetetty tai vastaanotettu Block ACK -sopimuksen alaisena. Arvo voi olla välillä **0** - **65535** ms. Oletus on **0**, mikä poistaa aikakatkaisun käytöstä.

Aggregation Window Size (Aggregoinnin ikkunakoko) Määrittää ilman ACK-kuittauksia siirrettävien pakettien enimmäismäärän. Arvo voi olla välillä **0** - **64**. Oletus on **64**.

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Wireless (Langaton verkko) > Advanced Wireless Settings (Langattoman verkon lisäasetukset)

Määritä sillan langattoman verkon lisäasetukset. Vain asiantuntevan järjestelmänvalvojan tulisi muuttaa näitä asetuksia, sillä väärät asetukset voivat heikentää langattoman verkon toimivuutta.



HUOMAUTUS
Advanced Wireless Settings (Langattoman verkon lisäasetukset) -näytön asetukset on tarkoitettu vain edistyneille käyttäjille.

Advanced Wireless (Langattoman verkon lisäasetukset)

Use LDPC (Käytä LDPC:tä) LDPC (Low-Density Parity-Check Code) ottaa käyttöön tai poistaa käytöstä virheiden korjauksen tietojen menettämisen todennäköisyyden pienentämiseksi noisy channel -oloissa. Rate Adaptation -algoritmi poistaa LDPC-koodauksen automaattisesti käytöstä, kun työskennellään korkeilla PHY-nopeuksilla (yli 162). Jos haluat käyttää edistynyttä LDCP-virheiden korjausta, älä muuta oletusasetusta **Yes** (Kyllä). Valitse muussa tapauksessa **No** (Ei).

ERP Protection Type (ERP-suojaustyyppi) Määrittää OFDM-pakettien suojauksen riippumatta 802.11b-kanavien läsnäolosta langattomassa verkossa. Lähettämällä RTS/CTS- tai CTS2Self-paketteja 802.11b-nopeuksilla silta kertoo langattomalle verkolle, että OFDM-paketteja aiotaan lähettää, ja suojelee paketteja langattomassa verkossa. RTS/CTS- ja CTS2Self-paketit luovat yleisrasitusta, joka saattaa hidastaa tiedonsiirtoa.

RTS/CTS-vaihtoehto tarjoaa parempaa kattavuutta, mutta hitaampaa tiedonsiirtoa kuin CTS2Self, sillä RTS/CTS pyytää kuittauksen vastaanottavalta laitteelta. Jos haluat käyttää RTS/CTS-vaihtoehtoa, älä muuta oletusasetusta **RTS/CTS**. Vaihtoehto None (Ei mitään) saattaa aiheuttaa törmäyksiä OFDM- ja CCK-pakettien välillä. Jos haluat käyttää vaihtoehtoa None (Ei mitään), valitse **None** (Ei mitään). Jos haluat käyttää vaihtoehtoa CTS2Self, valitse **CTS2Self**.

11n Protection Type (11n-suojaustyyppi) Määrittää HT (non-High Throughput) -laitteiden suojauksen langattomassa verkossa. Jos langaton reititin (tai yhteyspiste) havaitsee vanhemman ei-HT-laitteen, se kehottaa kaikkia HT-laitteita käyttämään RTS/CTS- tai CTS2Self-mekanismia ennen jokaista tiedonsiirtoa. Toiminto tukee myös kaikkia 802.11n-standardisuojauksia, mukaan lukien MIMO.

RTS/CTS-vaihtoehto tarjoaa parempaa kattavuutta, mutta hitaampaa tiedonsiirtoa kuin CTS2Self, sillä RTS/CTS pyytää kuittauksen vastaanottavalta laitteelta. Jos haluat käyttää RTS/CTS-vaihtoehtoa, älä muuta oletusasetusta **RTS/CTS**. Vaihtoehto None (Ei mitään) saattaa aiheuttaa törmäyksiä HT-pakettien ja vanhempien pakettien välillä. Jos haluat käyttää vaihtoehtoa None (Ei mitään), valitse **None** (Ei mitään). Jos haluat käyttää vaihtoehtoa CTS2Self, valitse **CTS2Self**.

Percentage of maximal transmit power (Siiron enimmäisteho prosentteina) Määrittää siirron enimmäistehon prosentteina suhteessa toimialueen säädösten mukaisiin rajoituksiin. Jos esimerkiksi toimialueen säädökset sallivat enintään 20 dB:n lähetyksen ja asetukseksi on määritetty 50 %, siirron sallittu enimmäisteho on 10 dB. Valitse haluamasi prosenttiosuus: **12 %**, **25 %**, **50 %** tai **100 %**. Oletus on **100%**.

QoS Classification Type (QoS-luokittelutyyppi) Määrittää 802.1D- tai 802.1Q-määrityksen IP DSCP/TOS -kentästä WMM-prioriteetteihin (Background (Tausta), Best Effects (Parhaat efektit), Video (Video), Voice (Ääni)). Pidä oletus **802.1D** tai valitse **802.1Q**, jota käytetään joissakin IPTV-stream-siirroissa.

Re-establish Ethernet connection when initiating wireless connection (Luo Ethernet-yhteys uudelleen, kun langaton yhteys muodostetaan) Käynnistääkseen sillan takana olevan laitteen DHCP-etsinnän silta luo uudelleen Ethernet-yhteyden sen ja laitteen välille aina, kun langaton yhteys muodostetaan. Voit poistaa toiminnon käytöstä valitsemalla **No** (Ei). Muutoin pidä oletus **Yes** (Kyllä).

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Administration (Valvonta) > Management (Hallinta)

Tällä näytöllä voit hallita tiettyjä sillan toimintoja: pääsyä -selainapuohjelmaan, määritystiedoston varmuuskopiointia ja uudelleen käynnistämistä.



Management (Hallinta)

Bridge Access (Sillan käyttö)

Suojaa selainapuohjelman käyttö salasanalla.

Bridge Password (Sillan salasana) Anna sillalle uusi salasana.

Re-enter to confirm (Vahvista antamalla uudelleen) Vahvista salasana kirjoittamalla se uudelleen.

Idle Timeout (Lepotilan aikakatkaisu) Selain kirjautuu ulos apuohjelmasta määritellyn käyttämättömyysajan jälkeen. Arvo voi olla välillä **60** - **3600** sekuntia. Oletus on **600**.

Web Access (Web-käyttö)

Access via Wireless (Käyttö langattoman verkon kautta) Jos käytät siltaa julkisella toimialueella, jossa vieraat käyttävät langatonta yhteyttä, voit kieltää selainapuohjelman käytön. Tällöin selainapuohjelmaa voi käyttää vain kiinteän verkon kautta. Jos haluat, että sillan selainapuohjelmaa voi käyttää langattoman verkon kautta, jätä käyttöön oletusasetus **Enabled** (Käytössä). Jos haluat estää käytön langattoman verkon kautta, valitse **Disabled** (Ei käytössä).

Backup and Restore (Varmuuskopiointi ja palautus)

Backup (Varmuuskopiointi) Voit tehdä varmuuskopion sillan asetustiedostosta valitsemalla **Backup Configurations** (Varmuuskopioi asetukset). Seuraa sitten näyttöön avautuvia ohjeita.

Restore (Palautus) Valitse **Browse** (Selaa) ja sitten asetustiedosto. Valitse sitten **Restore Configurations** (Palauta asetukset).

System Reboot (Järjestelmän uudelleenkäynnistys)

Reboot (Käynnistä uudelleen) Käynnistä silta uudelleen valitsemalla **Start to Reboot** (aloita uudelleenkäynnistys).

Ota muutokset käyttöön valitsemalla **Save Settings** (Tallenna asetukset) tai peruuta muutokset valitsemalla **Cancel Changes** (Peruuta muutokset).

Administration (Valvonta) > Factory Defaults (Tehdasoletukset)

Tässä näytössä voit palauttaa sillan tehdasasetukset.

Factory Defaults (Tehdasoletukset)

Restore All Settings (Palauta kaikki asetukset) Palauta sillan asetukset tehdasoletuksiksi valitsemalla **Restore All Settings** (Palauta kaikki asetukset). Kaikki aiemmin määrittämäsi asetukset katoavat, kun tehdasasetukset palautetaan.



Administration (Valvonta) > Upgrade Firmware (Laiteohjelmiston päivitys)

Tässä näytössä voit päivittää sillan laiteohjelmiston. Päivitä laiteohjelmisto vain, jos sillassa on ongelmia tai uudessa laiteohjelmistossa on jokin ominaisuus, jota haluat käyttää.



Ennen kuin päivität laiteohjelmiston, lataa sillan laiteohjelmistopäivitystiedosto Linksysin web-sivustosta osoitteessa **www.Linksys.com/support**.

Upgrade Firmware (Laiteohjelmiston päivitys)

Please select a file to upgrade the firmware (Valitse tiedosto, joka sisältää laiteohjelmistopäivityksen) Valitse **Browse** (Selaa) ja valitse laiteohjelmistopäivitystiedosto. Valitse sitten **Start to Upgrade** (Aloita päivitys) ja seuraa näytön ohjeita.

Status (Tila) > Bridge (Silta)

Sillan nykyinen tila.



Bridge Information (Sillan tiedot)

Firmware Version (Laiteohjelmistoversio) Sillan nykyinen laiteohjelmistoversio.

Local Network (Lähiverkko)

Local MAC Address (Paikallinen MAC-osoite) Paikallisessa Ethernet-verkossa näkyvä sillan MAC-osoite.

IP Address (IP-osoite) Paikallisessa Ethernet-verkossa näkyvä sillan IP-osoite.

Subnet Mask (Aliverkon peite) Paikalliselle verkolle määritetty aliverkon peite.

Status (Tila) > Wireless (Langaton verkko)

Tietoja langattomasta verkosta.



Wireless (Langaton verkko)

Link Status (Yhteyden tila) Langattoman verkon yhteyden tila.

MAC Address (MAC-osoite) Paikallisessa langattomassa verkossa näkyvä sillan MAC-osoite.

Network Name (SSID) (Verkkonimi (SSID)) Langattoman verkon nimi eli SSID.

BSSID Kytketyn langattoman reitittimen (tai yhteyspisteen) langaton MAC-osoite.

Radio Band (Radiotaajuus) Langattoman verkon radiotaajuus.

Channel Width (Kanavan leveys) Langattoman verkon käyttämän kanavan leveys (MHz).

Wide Channel (Leveä kanava) Leveä kanava (riippuu verkkoreitittimen kanava-asetuksista). Jos reitittimen Radio Band (Radiokanava)- tai Channel Width (Kanavan leveys) -asetukseksi on valittu 40 MHz, tämä toimii ensisijaisena Wireless-N-kanavana.

Standard Channel (Vakiokanava) Vakiokanava-asetus. Jos reitittimen Radio Band (Radiokanava)- tai Channel Width (Kanavan leveys) -asetukseksi on valittu 40 MHz, vakiokanava toimii toissijaisena Wireless-N-kanavana.

Bit Rate (Bittinopeus) Tiedonsiirtonopeus.

Signal (Signaali) Signaalin voimakkuus prosentteina. 100 % on vahvin mahdollinen signaali, 0 % heikoin.

Suojaus Langattoman verkon suojausmetodi.

Vianmääritys

WES610N/WET610N

Tietokone tai muu johdollinen Ethernet-laite ei saa yhteyttä langattomaan reitittimeen.

1. Avaa sillan selainpohjainen apuohjelma.
2. Varmista, että *Basic Wireless Settings* (Langattoman verkon perusasetukset) -näytön Network Name (SSID) (Verkkonimi (SSID)) vastaa langattoman verkon nimeä.
3. Varmista, että suojausasetukset (WPA, WPA2 tai WEP) vastaavat langattoman verkon suojausasetuksia.

Sillan IP-osoite täytyy muuttaa.

Jos silta on liitetty verkkoon, jossa on DHCP-palvelin (yleensä verkkoreititin), silta saa IP-osoitteensa DHCP-palvelimelta. Jos verkossa ei ole DHCP-palvelinta, silta käyttää staattista oletus-IP-osoitetta **169.254.1.250**.

Jos haluat, että silta käyttää aina staattista IP-osoitetta, seuraa näitä ohjeita:

1. Avaa sillan selainpohjainen apuohjelma.
2. Avaa **Network Setup** (Verkon asetukset) -välilehti
3. Valitse *Network Connection Type* (Verkkoyhteyden tyyppi) -valikosta **Static IP** (Staattinen IP).
4. Täytä kentät *Static IP Address* (Staattinen IP-osoite), *Subnet Mask* (Aliverkon peite) ja *Default Gateway* (Oletusyhdyskäytävä).
5. Valitse **Save Settings** (Tallenna asetukset).

Tietokone, jossa on silta käytössä, tai muu johdollinen Ethernet-laite ei saa yhteyttä toiseen langattomaan laitteeseen (kuten tietokone tai tulostin).

Tee seuravat tarkistukset:

- Tarkista, että langaton laite on samassa langattomassa verkossa kuin siltaan liitetty tietokone tai muu johdollinen Ethernet-laite.
- Tarkista, että kaikkien langattomassa verkossa olevien laitteiden Network Name (SSID) (Verkkonimi (SSID) on sama.
- Tarkista, että kaikki laitteet ovat samassa IP-verkossa ja käyttävät yhteensopivia IP-osoitteita.

Selainpohjainen apuohjelma ei hyväksy salasanaasi.

Tee seuravat tarkistukset:

- Salasanan kirjainkoko on merkitsevä. Tarkista, että kirjoitat salasanan pienet ja isot kirjaimet oikein.
- Jos unohdat salasanan, voit palauttaa sillan tehdasasetukset.

 Pidä sillan **Reset**-painiketta painettuna noin viiden sekunnin ajan, niin salasana palautuu tehdasasetukseksi: **admin**. Sillan kaikki muut asetukset palautuvat myös oletusarvoisiksi. (Pääset selainpohjaiseen apuohjelmaan kirjoittamalla *Password* (Salasana) -kenttään "**admin**".)

Selainpohjaisessa apuohjelmassa tekemäsi muutokset asetuksiin eivät näy näytöllä.

Päivitä selain. Jos uudet asetukset eivät vieläkään näy, seuraa näitä ohjeita:

1. Irrota virtasovitin sillasta.
2. Odota viisi sekuntia ja kytke virtasovitin takaisin kiinni.
3. **Päivitä** selain.

WEB
Jos et saa vastausta kysymyksiisi näistä ohjeista, mene Linksysin sivustoon osoitteeseen **Linksys.com/support**

Tekniset tiedot

WES610N

Malli	WES610N
Standardit	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Merkkivalot	Virta, Ethernet, Wi-Fi Protected Setup™, langaton yhteys, yksittäinen Ethernet-linkki ja toiminta
Portit	Ethernet (4), virta
Painikkeet	Reset, Wi-Fi Protected Setup
Kaapelin tyyppi	CAT5e
Antennit	3 (sisäistä)
Antenniliittimen tyyppi	-
Irrotettava (kyllä/ei)	Ei
Modulaatiot	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP), dBm	802.11a: 15 dBm (tavallinen), 54 Mbps 802.11b: 19 dBm (tavallinen), 11 Mbps 802.11g: 16 dBm (tavallinen), 54 Mbps 802.11n (2.4 GHz): 18 dBm (tavallinen), MCS15 802.11n (5 GHz): 16 dBm (tavallinen), MCS15
Vastaanottoherkkyys	802.11a: -72 dBm (tavallinen), 54 Mbps 802.11b: -85 dBm (tavallinen), 11 Mbps 802.11g: -73 dBm (tavallinen), 54 Mbps 802.11n (20 MHz): -75 dBm (tavallinen), MCS15 802.11n (40 MHz): -69 dBm (tavallinen), MCS15
Antennivahvistus, dBi	1
Langattoman yhteyden suojaus	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Suojausavaimen pituus, bittiä	Jopa 128-bittinen salaus

Käyttöympäristötiedot

Mitat	177 x 128 x 68 mm
Paino	295 g
Sertifiointi	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Virta	12 V, 1 A
Käyttölämpötila	0...40 ºC)
Varastointilämpötila	-20...+60 °C
Käyttöympäristön ilmankosteus	10–85 %, kondensoitumaton
Varastointiympäristön ilmankosteus	5–90 %, kondensoitumaton

Tekniset tiedot voivat muuttua ilman erillistä ilmoitusta.

WET610N

Malli	WET610N
Standardit	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Merkkivalot	Virta, Ethernet, Wi-Fi Protected Setup™, langaton yhteys
Portit	Ethernet, virta
Painikkeet	Reset, Wi-Fi Protected Setup
Kaapelin tyyppi	CAT5e
Antennit	3 (sisäistä)
Antenniliittimen tyyppi	-
Irrotettava (kyllä/ei)	Ei
Modulaatiot	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP), dBm	802.11a: 15 dBm (tavallinen), 54 Mbps 802.11b: 18 dBm (tavallinen), 11 Mbps 802.11g: 16 dBm (tavallinen), 54 Mbps 802.11n: 12 dBm (tavallinen), 130 Mbps (HT20), 270 Mbps (HT40)
Vastaanottoherkkyys	802.11a: -72 dBm (tavallinen), 54 Mbps 802.11b: -85 dBm (tavallinen), 11 Mbps 802.11g: -73 dBm (tavallinen), 54 Mbps 802.11n: -70 dBm (tavallinen), MCS15/2.4 GHz, -69 dBm (tavallinen), MCS15/5.0 GHz
Antennivahvistus, dBi	1
Langattoman yhteyden suojaus	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Suojausavaimen pituus, bittiä	Jopa 128-bittinen salaus

Käyttöympäristötiedot

Mitat	145 x 106 x 52 mm
Paino	159 g
Sertifiointi	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Virta	12 V, 1 A
Käyttölämpötila	0...40 ºC)
Varastointilämpötila	-20...+60 °C
Käyttöympäristön ilmankosteus	10–85 %, kondensoitumaton
Varastointiympäristön ilmankosteus	5–90 %, kondensoitumaton

Tekniset tiedot voivat muuttua ilman erillistä ilmoitusta.

Linksys.com/support

Cisco, Cisco-logo ja Linksys ovat Ciscon ja/tai sen tytäryhtiöiden tavaramerkkejä tai rekisteröityjä tavaramerkkejä Yhdysvalloissa ja muissa maissa.
Luettelo Ciscon tavaramerkeistä on osoitteessa www.cisco.com/go/trademarks. Kaikki muut tässä asiakirjassa mainitut tavaramerkit ovat niiden omistajien omaisuutta.

© 2011 Cisco ja/tai sen tytäryhtiöt. Kaikki oikeudet pidätetään.

3425-01249



Guide de l'utilisateur

Linksys WET610N/WES610N | Pont N double bande grand public

Table des matières

Présentation du produit

Panneau des voyants 2
Panneau des ports. 3

Liste de vérification de la sécurité sans fil

Modifier le nom ou SSID du réseau sans fil par défaut 4
Modifier le mot de passe par défaut 4
Activer le filtrage des adresses MAC 4
Activer le cryptage 4

Consignes de sécurité réseau d'ordre général 4
Consignes de sécurité supplémentaires 5

Configuration avancée

Comment accéder à l'utilitaire basé sur le navigateur Web ? . . . 6
Configuration > Configuration de base 7
Langue 7
Configuration réseau 7
Sans fil > Paramètres sans fil de base 7
Paramètres sans fil de base 8
Sécurité sans fil 8
Wi-Fi Protected Setup 9
Sans fil > Recherche de site réseau sans fil. 10
Recherche de site de réseau sans fil 10
Sans fil > WMM® 11
WMM 12
Sans fil > Paramètres sans fil avancés 13
Paramètres sans fil avancés 13
Administration > Gestion 14
Gestion 14
Administration > Paramètres d'usine 15
Paramètres d'usine 15
Administration > Mise à niveau du micrologiciel 15
Mise à niveau du micrologiciel 15
Etat > Pont. 15
Informations concernant le pont 16
Réseau local 16
Etat > Sans fil 16
Sans fil 16

Dépannage

WES610N/WET610N 17

Spécifications

WES610N 18
WET610N 19

Présentation du produit

Merci d'avoir choisi le pont N double bande grand public de Linksys. Ce pont permet de relier à votre réseau sans fil n'importe quel périphérique câblé Ethernet. Il est basé sur la technologie sans fil N double bande, et par conséquent compatible avec tout point d'accès ou routeur sans fil N, G, A ou B. Lors de la première installation, suivez les instructions fournies dans le dossier du CD. Pour configurer des paramètres avancés, recourez à l'utilitaire très pratique basé sur votre navigateur.

Panneau des voyants



WES610N WET610N

Sans fil (bleu) : ce voyant s'allume lorsqu'une connexion sans fil est établie. Le voyant clignote lorsque le pont envoie ou reçoit activement des données sur le réseau sans fil.

Bouton Wi-Fi Protected Setup : si votre routeur prend en charge cette fonction et utilise la sécurité WPA ou WPA2, vous pouvez utiliser la fonctionnalité Wi-Fi Protected Setup pour connecter automatiquement le pont. Avant d'utiliser la fonctionnalité Wi-Fi Protected Setup, reportez-vous à « Sans fil > Paramètres sans fil de base » à la page 7.

Voyant Wi-Fi Protected Setup (bleu/orange) : le voyant clignote en bleu pendant deux minutes lors du processus Wi-Fi Protected Setup. Il s'allume en bleu lorsque la sécurité sans fil est activée. En cas d'erreur durant le processus Wi-Fi Protected Setup, le voyant s'allume en orange. Assurez-vous que le routeur réseau prend en charge la fonctionnalité Wi-Fi Protected Setup. Attendez que le voyant s'éteigne, puis réessayez.

Ethernet (bleu) : ce voyant s'allume lorsqu'une connexion câblée est établie. Le voyant clignote lorsque le pont envoie ou reçoit activement des données sur le ou les ports Ethernet.

Alimentation (bleu) : ce voyant s'allume lorsque le pont est sous tension.

Panneau des ports



WES610N WET610N

Ethernet : le ou les ports Ethernet connectent le pont à un ordinateur ou à un autre périphérique réseau Ethernet. Le modèle WES610N dispose de quatre ports, tandis que le WET610N ne possède qu'un seul port.

Réinitialisation : il existe deux façons de rétablir les paramètres par défaut d'usine du pont. Appuyez sur le bouton Reset (Réinitialisation) pendant environ cinq secondes ou restaurez les paramètres par défaut à partir de l'écran Administration > Factory Defaults (Administration > Paramètres d'usine) de l'utilitaire basé sur le Web du pont. Le bouton de réinitialisation du modèle WES610N est placé en bas du pont et celui du WET610N est positionné sur le panneau des ports arrière.

Alimentation : ce port permet de connecter le pont à l'adaptateur électrique fourni.

Liste de vérification de la sécurité sans fil

Très pratiques et d'une grande simplicité d'installation, les réseaux sans fil sont de plus en plus souvent choisis par les foyers disposant d'une connexion Internet haut débit. Toutefois, l'utilisation d'ondes radio rend les réseaux sans fil plus vulnérables que les réseaux câblés traditionnels. De la même façon qu'il est possible d'intercepter les signaux de votre téléphone cellulaire ou sans fil, les signaux de votre réseau sans fil peuvent également être interceptés. Etant donné qu'il est impossible de bloquer physiquement une connexion non autorisée à votre réseau sans fil, certaines mesures sont nécessaires pour garantir la sécurité de votre réseau.

Modifier le nom ou SSID du réseau sans fil par défaut

Tout périphérique sans fil possède un nom de réseau sans fil ou SSID (Service Set Identifier) configuré en usine. Il s'agit du nom de votre réseau sans fil ; il peut comporter jusqu'à 32 caractères. Les produits sans fil Linksys utilisent **linksys** comme nom de réseau sans fil par défaut. Il est recommandé de changer le nom de votre réseau sans fil pour le différencier des autres réseaux sans fil, mais n'utilisez pas d'informations personnelles (telles que votre numéro de téléphone), car ces informations sont disponibles à toute personne à la recherche de réseaux sans fil.

Modifier le mot de passe par défaut

Pour les produits sans fil, tels que les points d'accès et les routeurs, un mot de passe vous est demandé si vous souhaitez modifier leurs paramètres. Ces périphériques possèdent un mot de passe par défaut configuré en usine. Le mot de passe Linksys par défaut est **admin**. Les pirates informatiques connaissent ces noms et peuvent tenter d'accéder à votre réseau sans fil et de modifier vos paramètres réseau. Pour éviter toute modification non autorisée, personnalisez le mot de passe du périphérique de sorte qu'il soit difficile à deviner.

Activer le filtrage des adresses MAC

Les routeurs Linksys permettent d'activer le filtrage d'adresses MAC (Media Access Control). Tout périphérique réseau se voit attribuer une adresse MAC unique, composée d'une série de chiffres et de lettres. Lorsque la fonction de filtrage des adresses MAC est activée, l'accès au réseau sans fil n'est autorisé qu'aux périphériques dont l'adresse MAC est reconnue. Vous pouvez, par exemple, spécifier l'adresse MAC de chaque ordinateur de votre domicile, de manière à ce que seuls ces ordinateurs puissent accéder au réseau sans fil.

Activer le cryptage

Le cryptage protège les données transmises via un réseau sans fil. WPA/WPA2 (Wi-Fi Protected Access) et WEP (Wired Equivalent Privacy) offrent différents niveaux de protection des communications sans fil.

Un réseau utilisant le cryptage WPA/WPA2 est plus sécurisé qu'un réseau utilisant le cryptage WEP, car WPA/WPA2 utilise une méthode de cryptage par clé dynamique. Afin de protéger les informations transmises par ondes radio, il est recommandé d'activer le niveau de cryptage le plus élevé pris en charge par votre matériel réseau.

Il est possible que les périphériques les plus anciens, qui ne prennent pas en charge la sécurité WPA, ne proposent que la méthode de cryptage WEP.

Consignes de sécurité réseau d'ordre général

La sécurité du réseau sans fil ne sert à rien si le réseau sous-jacent n'est pas sécurisé.

- Protégez l'accès à tous les ordinateurs du réseau à l'aide de mots de passe et protégez vos fichiers importants à l'aide de mots de passe individuels.
- Modifiez les mots de passe régulièrement.
- Installez un logiciel anti-virus et un pare-feu personnel sur chaque poste.
- Désactivez le partage de fichiers (point à point). Certaines applications sont susceptibles de partager des fichiers sans demande de confirmation ou avertissement.

Consignes de sécurité supplémentaires

- Maintenez routeurs, points d'accès et modems routeurs sans fil à distance des murs extérieurs ou des fenêtres.
- Mettez hors tension les routeurs, points d'accès ou modems routeurs lorsqu'ils ne sont pas utilisés (la nuit, pendant vos vacances).
- Utilisez des phrases de passe d'au moins huit caractères et difficiles à deviner. Mélangez chiffres et lettres pour éviter tout mot pouvant se trouver dans un dictionnaire.

Configuration avancée

Après l'avoir configuré en suivant les instructions fournies dans le dossier du CD, le pont sera prêt à l'emploi. Cependant, si vous souhaitez modifier ses paramètres avancés, utilisez l'utilitaire basé sur le navigateur Web du pont. Ce chapitre décrit chaque page Web de l'utilitaire ainsi que ses fonctions clés. Vous pouvez accéder à l'utilitaire à l'aide d'un navigateur Web sur un ordinateur connecté au pont par réseau.

L'utilitaire basé sur le navigateur Web dispose des onglets principaux suivants : Setup (Configuration), Wireless (Sans fil), Administration et Status (Etat). D'autres onglets apparaissent lorsque vous cliquez sur les onglets principaux.

Comment accéder à l'utilitaire basé sur le navigateur Web ?

Utilisez un navigateur Web pour accéder à l'utilitaire basé sur le navigateur Web.

Si le pont est connecté à un réseau avec un serveur DHCP (généralement le routeur réseau), il obtient son adresse IP auprès du serveur DHCP. En l'absence de serveur DHCP, le pont utilise son adresse IP statique par défaut, **169.254.1.250**. (Si vous avez défini une adresse IP statique permanente sur le pont par l'intermédiaire de l'utilitaire basé sur le navigateur Web, entrez l'adresse IP statique.)

REMARQUE
Si vous ne connaissez pas l'adresse IP du pont, consultez la table des clients DHCP de votre routeur. (Voir la documentation de votre routeur.)

Si vous n'arrivez pas à trouver l'adresse IP du pont, vous pouvez le réinitialiser ; appuyez sur son bouton **Reset** (Réinitialisation) pendant environ cinq secondes à l'aide d'un trombone détendu. Ceci rétablit ses paramètres d'usine par défaut. Le pont demande alors une adresse IP au serveur DHCP (généralement le routeur réseau). Si le serveur DHCP est introuvable, le pont utilise son adresse IP statique par défaut, **169.254.1.250**, jusqu'à ce qu'il détecte un serveur DHCP et qu'une adresse IP dynamique lui soit affectée.

Si le pont n'est pas associé à un routeur et utilise les paramètres d'usine par défaut, connectez un ordinateur au pont à l'aide d'une connexion Ethernet pour accéder à l'utilitaire basé sur le navigateur Web. Vous devrez configurer la connexion Ethernet sur l'ordinateur avec une adresse IP statique et un masque de sous-réseau.

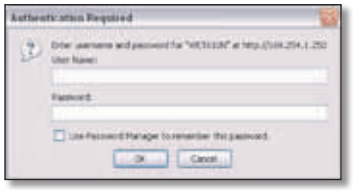
L'adresse IP de votre adaptateur Ethernet doit être définie sur une adresse IP spécifique.

1. Dans le champ *IP address* (Adresse IP), entrez **169.254.x.y** (x doit être remplacé par un chiffre de 1 à 254, et y par un chiffre de 0 à 255).
2. Dans le champ *Subnet mask* (Masque de sous-réseau), entrez **255.255.0.0**.

REMARQUE
La procédure d'affectation d'une adresse IP statique à l'adaptateur Ethernet de votre ordinateur varie suivant le système d'exploitation. Pour obtenir des instructions, reportez-vous à la documentation d'aide propre à votre système d'exploitation.

Après affectation d'une adresse IP statique à votre adaptateur Ethernet, lancez votre navigateur Web et entrez l'adresse IP de l'adaptateur (le paramètre par défaut est **169.254.1.250**) dans le champ *Address* (Adresse). Appuyez sur **Enter** (Entrée).

Un écran vous invite à entrer un mot de passe. (Les utilisateurs non-Windows XP obtiendront un écran similaire.) Ne remplissez pas le champ *User name* (Nom d'utilisateur). Entrez le mot de passe créé avec l'Assistant de configuration. Si vous n'avez pas créé de nouveau mot de passe, utilisez le mot de passe par défaut **admin**. (Vous pouvez définir un nouveau mot de passe à partir de l'écran *Administration* > *Management* (Administration > Gestion).) Cliquez sur **OK** pour continuer.



REMARQUE
Si l'écran de demande de mot de passe ne s'affiche pas, attendez deux minutes et réessayez.

Configuration > Configuration de base

Le premier écran qui s'affiche est l'écran *Basic Setup* (Configuration de base). Utilisez cet écran pour modifier la langue de l'utilitaire basé sur le navigateur Web ou les paramètres de réseau Ethernet câblé du pont.





Langue

Language (Langue) : permet de configurer la langue affichée par l'utilitaire basé sur le navigateur Web. Sélectionnez la langue de votre choix dans le menu déroulant.

Configuration réseau

Cette section détermine si l'adresse IP du pont est obtenue automatiquement à partir d'un serveur DHCP, tel que votre routeur réseau (Configuration automatique - DHCP), ou définie manuellement (IP statique).

Bridge IP (Adresse IP du pont) : si votre réseau comporte un serveur DHCP, tel que votre routeur réseau, attribuant des adresses IP à vos périphériques réseau, conservez la valeur par défaut, **Automatic Configuration - DHCP** (Configuration automatique - DHCP). Le pont demande alors une adresse IP au serveur DHCP (généralement le routeur réseau). Si le serveur DHCP est introuvable, le pont utilise son adresse IP statique par défaut, **169.254.1.250**, jusqu'à ce qu'il détecte un serveur DHCP et qu'une adresse IP dynamique lui soit affectée.

Si vous souhaitez définir une adresse IP statique permanente pour le pont, sélectionnez **Static IP** (Adresse IP statique).

Dans ce cas, complétez les champs suivants :

- **Static IP Address** (Adresse IP statique) : entrez une adresse IP unique qui sera utilisée pour accéder à l'utilitaire basé sur le navigateur Web.
- **Subnet Mask** (Masque de sous-réseau) : entrez le masque de sous-réseau de votre réseau câblé.
- **Default Gateway** (Passerelle par défaut) : entrez l'adresse IP de la passerelle par défaut de votre réseau (dans la plupart des cas, il s'agit de votre routeur).

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Sans fil > Paramètres sans fil de base

Utilisez l'écran *Basic Wireless Settings* (Paramètres sans fil de base) pour configurer les paramètres de sécurité et sans fil du pont.

Deux procédures permettent de configurer les paramètres du pont : la configuration manuelle et le Wi-Fi Protected Setup (Configuration protégée par Wi-Fi). Wi-Fi Protected Setup (Configuration protégée par Wi-Fi) est une fonction qui facilite la configuration de votre réseau sans fil. Si votre routeur réseau prend en charge cette fonction et utilise la sécurité WPA ou WPA2, vous pouvez utiliser le Wi-Fi Protected Setup pour connecter automatiquement le pont.

Configuration View (Affichage de la configuration) : pour configurer votre réseau sans fil manuellement, sélectionnez **Manual** (Manuel). Reportez-vous à la section **Paramètres sans fil de base**, **page 8**. Pour utiliser le Wi-Fi Protected Setup, sélectionnez **Wi-Fi Protected Setup**. Reportez-vous à la section **Wi-Fi Protected Setup**, **page 9**.

Paramètres sans fil de base



Network Name (SSID) (Nom du réseau (SSID)) : le SSID est le nom de réseau partagé par tous les points d'un réseau sans fil. Il doit être identique pour tous les périphériques du réseau sans fil. Ce paramètre tient compte de la casse et ne doit pas comprendre plus de 32 caractères. Tous les caractères du clavier peuvent être utilisés. Assurez-vous que ce paramètre correspond à celui défini sur votre routeur sans fil ou point d'accès. Pour optimiser la sécurité de votre système, vous devez remplacer le nom du réseau sans fil par défaut (**linksys**) par un nom unique.

Sécurité sans fil

Le pont prend en charge les options de sécurité sans fil suivantes : WPA Personal (WPA personnel) et WPA2 Personal, (WPA2 personnel) et WEP. WPA (Wi-Fi Protected Access) et WPA2 constituent des normes de sécurité plus puissantes que WEP (Wired Equivalent Privacy). Pour en savoir plus sur la sécurité sans fil, reportez-vous à la section « Liste de vérification de la sécurité sans fil », page 4.

Security Mode (Mode de sécurité)

Sélectionnez la méthode de sécurité pour votre réseau sans fil. Si vous ne souhaitez pas utiliser cette fonction, conservez l'option par défaut, **Disabled** (Désactivé).

REMARQUE
Rappelez-vous que chaque périphérique de votre réseau sans fil DOIT utiliser les mêmes méthode de sécurité et phrase de passe/clé. Dans le cas contraire, les périphériques sans fil ne peuvent pas communiquer entre eux.

WPA Personal (WPA personnel)

WPA désigne une norme de sécurité plus puissante que le système de cryptage WEP.



Encryption (Cryptage) : WPA prend en charge la méthode de cryptage TKIP, avec des clés de cryptage dynamiques.

Passphrase (Phrase de passe) : saisissez la clé partagée par le pont et votre routeur sans fil ou point d'accès. Elle doit comporter entre 8 et 63 caractères.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

WPA2 Personal (WPA2 personnel)

WPA2 est une version plus avancée et plus sécurisée de WPA.



Encryption (Cryptage) : WPA2 prend en charge deux méthodes de cryptage, nommées TKIP et AES, associées à des clés de cryptage dynamiques. Sélectionnez la méthode de cryptage **AES** ou **TKIP or AES** (TKIP ou AES). La sélection par défaut est **AES**.

Passphrase (Phrase de passe) : saisissez la clé partagée par le pont et le routeur sans fil ou point d'accès. Elle doit comporter entre 8 et 63 caractères.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

WEP

Le système WEP est une méthode de cryptage élémentaire qui n'est pas aussi sûre que le système WPA ou WPA2.



Encryption (Cryptage) : sélectionnez un niveau de cryptage WEP, **40/64 bits (10 hex digits)** (40/64 bits [10 chiffres hexadécimaux]) ou **104/128 bits (26 hex digits)** (104/128 bits [26 chiffres hexadécimaux]). Le niveau de cryptage par défaut est **40/64 bits (10 hex digits)** (40/64 bits [10 chiffres hexadécimaux]).

Key 1 (Clé 1) : saisissez la clé WEP de votre réseau.

Tx Key (Clé de transmission) : **Key 1** (Clé 1) est la clé de transmission utilisée par le pont.

Authentication (Authentification) : la valeur **Auto** définie par défaut permet de choisir entre une authentification système ouvert ou par clé partagée. Sélectionnez **Open** (Ouvert) pour utiliser une authentification système ouvert ; l'expéditeur et le destinataire n'utilisent pas de clé WEP pour l'authentification. Sélectionnez **Shared** (Partagé) pour utiliser une authentification par clé partagée ; l'expéditeur et le destinataire utilisent une clé WEP pour l'authentification.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Wi-Fi Protected Setup

Deux méthodes sont disponibles. Utilisez la méthode qui s'applique au routeur que vous employez.





Méthode n° 1

Utilisez cette méthode si votre routeur dispose d'un bouton Wi-Fi Protected Setup.

1. Cliquez ou appuyez sur le bouton **Wi-Fi Protected Setup** (Configuration protégée par Wi-Fi) du routeur.
2. Vous disposez de deux minutes pour cliquer sur le bouton **Wi-Fi Protected Setup** (Configuration protégée par Wi-Fi) de l'écran *Wi-Fi Protected Setup* du pont.
3. Une fois le pont configuré, cliquez sur **Close** (Fermer).

L'écran *Wi-Fi Protected Setup* (Configuration protégée par Wi-Fi) affiche l'état de la liaison, le nom réseau (SSID) et la méthode de sécurité.

Méthode n°2

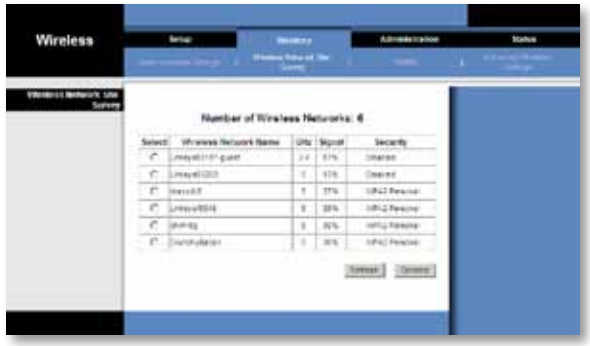
Utilisez cette méthode si votre routeur demande le code PIN du pont.

1. Dans l'écran *Wi-Fi Protected Setup* (Configuration protégée par Wi-Fi) du **routeur**, saisissez le code PIN de l'écran correspondant sur le **pont**. Cliquez ensuite sur **Register** (Enregistrement) ou sur le bouton approprié. (Ce code est également noté sous le pont.)
2. Dans l'écran *Wi-Fi Protected Setup* (Configuration protégée par Wi-Fi) du **pont**, cliquez sur **OK**.
3. Une fois le pont configuré, cliquez sur **Close** (Fermer).

L'écran *Wi-Fi Protected Setup* (Configuration protégée par Wi-Fi) affiche l'état de la liaison, le nom réseau (SSID) et la méthode de sécurité.

Sans fil > Recherche de site réseau sans fil

Cliquez sur l'onglet **Wireless Network Site Survey** (Recherche de site réseau sans fil) pour lancer une recherche de site. L'écran *Wireless Network Site Survey* (Recherche de site réseau sans fil) répertorie les réseaux sans fil détectés par le pont.



Recherche de site de réseau sans fil

Number of Wireless Networks (Nombre de réseaux sans fil) : le nombre de réseaux sans fil détectés par le pont est affiché.

Select (Sélectionner) : cliquez sur **Select** (Sélectionner) pour vous connecter à un réseau sans fil. Cliquez ensuite sur **Connect** (Connexion).

Wireless Network Name (Nom du réseau sans fil) : le nom réseau ou SSID du réseau sans fil est affiché.

GHz : indique la bande radio du réseau sans fil.

Signal : correspond au pourcentage d'intensité du signal. 100 % indique l'intensité maximale ; 0 % identifie le niveau le plus faible.

Security (Sécurité) : si le réseau prend en charge le Wi-Fi Protected Setup, l'icône correspondante apparaît. La méthode de sécurité utilisée par le réseau sans fil est indiquée.

Cliquez sur le bouton **Refresh** (Actualiser) pour mettre à jour les informations à l'écran.

Après avoir sélectionné un réseau, cliquez sur **Connect** (Connexion). Un nouvel écran s'affiche. Suivez les instructions pour la méthode de sécurité de votre réseau.

WPA



Network Name (SSID) (Nom du réseau (SSID)) : le nom du réseau sélectionné est automatiquement affiché.

Security Mode (Mode de sécurité) : WPA Personal (WPA personnel) est automatiquement indiqué.

Encryption (Cryptage) : WPA prend en charge la méthode de cryptage TKIP, avec des clés de cryptage dynamiques.

Passphrase (Phrase de passe) : saisissez la clé partagée par le pont et le routeur sans fil ou point d'accès. Elle doit comporter entre 8 et 63 caractères.

Cliquez sur le bouton **Refresh** (Actualiser) pour mettre à jour les informations à l'écran.

Une fois les paramètres de sécurité renseignés, cliquez sur **Connect** (Connexion).

WPA2



Network Name (SSID) (Nom du réseau (SSID)) : le nom du réseau sélectionné est automatiquement affiché.

Security Mode (Mode de sécurité) : WPA2 Personal (WPA2 personnel) est automatiquement indiqué.

Encryption (Cryptage) : WPA2 prend en charge deux méthodes de cryptage, nommées TKIP et AES, associées à des clés de cryptage dynamiques. Sélectionnez la méthode de cryptage **AES** ou **TKIP or AES** (TKIP ou AES).

Passphrase (Phrase de passe) : saisissez la clé partagée par le pont et le routeur sans fil ou point d'accès. Elle doit comporter entre 8 et 63 caractères.

Cliquez sur le bouton **Refresh** (Actualiser) pour mettre à jour les informations à l'écran.

Une fois les paramètres de sécurité renseignés, cliquez sur **Connect** (Connexion).

WEP



Network Name (SSID) (Nom du réseau (SSID)) : le nom du réseau sélectionné est automatiquement affiché.

Security Mode (Mode de sécurité) : WEP est automatiquement indiqué.

Encryption (Cryptage) : sélectionnez un niveau de cryptage WEP, **40/64 bits (10 hex digits)** (40/64 bits [10 chiffres hexadécimaux]) ou **104/128 bits (26 hex digits)** (104/128 bits [26 chiffres hexadécimaux]).

Key 1 (Clé 1) : saisissez la clé WEP de votre réseau.

Tx Key (Clé de transmission) : **Key 1** (Clé 1) est la clé de transmission utilisée par le pont.

Authentication (Authentification) : la valeur **Auto** définie par défaut permet de choisir entre une authentification système ouvert ou par clé partagée. Sélectionnez **Open** (Ouvert) pour utiliser une authentification système ouvert ; l'expéditeur et le destinataire n'utilisent pas de clé WEP pour l'authentification. Sélectionnez **Shared** (Partagé) pour utiliser une authentification par clé partagée ; l'expéditeur et le destinataire utilisent une clé WEP pour l'authentification.

Cliquez sur le bouton **Refresh** (Actualiser) pour mettre à jour les informations à l'écran.

Une fois les paramètres de sécurité renseignés, cliquez sur **Connect** (Connexion).

Sans fil > WMM®

Configurez les paramètres WMM (Wireless MultiMedia). WMM définit la priorité des paquets suivant leur mode d'accès respectif (type de trafic) : Background (Arrière-plan), Best Effort (Effort maximum), Video (Vidéo) ou Voice (Voix). Il est préférable de réserver cette tâche à un administrateur chevronné, car des paramètres mal définis risqueraient de diminuer les performances de votre infrastructure sans fil.



REMARQUE
Les paramètres de l'écran *WMM* sont réservés aux utilisateurs avancés.

WMM

Mode d'accès

Vous pouvez attribuer différents paramètres aux quatre modes d'accès disponibles. Sélectionnez le mode que vous souhaitez configurer. **Background** (Arrière-plan), **Best Effort** (Effort maximum), **Video** (Vidéo) ou **Voice** (Voix). Suivez les instructions pour le mode sélectionné.

Arrière-plan

Use Aggregation (Utiliser l'agrégation) : cette option définit si la couche MAC (Media Access Control) configure une session ADDBA (Add Block Acknowledgement). **No** (Non) est l'option par défaut. Sélectionnez **Yes** (Oui) pour activer cette option.

Accept Aggregation (Accepter l'agrégation) : cette option définit si la couche MAC acceptera une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre maximum de paquets dans l'agrégation) : cette option définit le nombre maximum de paquets (sous-trames) dans l'agrégat. Ce nombre peut être compris entre **0** et **7**. La valeur par défaut est **7**.

Max. Aggregation Size (Taille maximale de l'agrégation) : cette option définit la taille maximale de l'agrégat (en octets). Ce nombre peut être compris entre **0** et **16 000**. La valeur par défaut est **12 000**.

Timeout Interval (Délai d'attente) : cette option définit la période d'attente au cours de laquelle l'agrégat doit être fermé avec une condition de clôture avant fermeture par la minuterie. Ce nombre peut être compris entre **0** et **100** ms. La valeur par défaut est **3**.

Min. Size of Packet in Aggregation (Taille minimum de paquet dans l'agrégation) : cette option définit la taille minimale (en octets) des paquets à cumuler dans l'agrégat. Ce nombre peut être compris entre **0** et **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai d'attente ADDBA) : cette option définit la durée au-delà de laquelle la configuration ADDBA est terminée, en l'absence d'échanges de trame dans ce délai par l'accord ACK (Block Acknowledgement, confirmation de bloc). Ce nombre peut être compris entre **0** et **65 535** ms. La valeur par défaut est **0**, ce qui désactive le délai d'attente.

Aggregation Window Size (Taille de la fenêtre d'agrégation) : cette option définit le nombre maximum de paquets transmis sans obtenir de confirmations. Ce nombre peut être compris entre **0** et **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Best Effort (Effort maximum)

Use Aggregation (Utiliser l'agrégation) : cette option définit si la couche MAC (Media Access Control) configure une session ADDBA (Add Block Acknowledgement). La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Accept Aggregation (Accepter l'agrégation) : cette option définit si la couche MAC acceptera une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre maximum de paquets dans l'agrégation) : cette option définit le nombre maximum de paquets (sous-trames) dans l'agrégat. Ce nombre peut être compris entre **0** et **10**. La valeur par défaut est **10**.

Max. Aggregation Size (Taille maximale de l'agrégation) : cette option définit la taille maximale de l'agrégat (en octets). Ce nombre peut être compris entre **0** et **20 000**. La valeur par défaut est **16 000**.

Timeout Interval (Délai d'attente) : cette option définit la période d'attente au cours de laquelle l'agrégat doit être fermé avec une condition de clôture avant fermeture par la minuterie. Ce nombre peut être compris entre **0** et **100** ms. La valeur par défaut est **3**.

Min. Size of Packet in Aggregation (Taille minimum de paquet dans l'agrégation) : cette option définit la taille minimale (en octets) des paquets à cumuler dans l'agrégat. Ce nombre peut être compris entre **0** et **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai d'attente ADDBA) : cette option définit la durée au-delà de laquelle la configuration ADDBA est terminée, en l'absence d'échanges de trame dans ce délai par l'accord ACK (Block Acknowledgement, confirmation de bloc). Ce nombre peut être compris entre **0** et **65 535** ms. La valeur par défaut est **0**, ce qui désactive le délai d'attente.

Aggregation Window Size (Taille de la fenêtre d'agrégation) : cette option définit le nombre maximum de paquets transmis sans obtenir de confirmations. Ce nombre peut être compris entre **0** et **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Vidéo

Use Aggregation (Utiliser l'agrégation) : cette option définit si la couche MAC (Media Access Control) configure une session ADDBA (Add Block Acknowledgement). La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Accept Aggregation (Accepter l'agrégation) : cette option définit si la couche MAC acceptera une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre maximum de paquets dans l'agrégation) : cette option définit le nombre maximum de paquets (sous-trames) dans l'agrégat. Ce nombre peut être compris entre **0** et **7**. La valeur par défaut est **7**.

Max. Aggregation Size (Taille maximale de l'agrégation) : cette option définit la taille maximale de l'agrégat (en octets). Ce nombre peut être compris entre **0** et **16 000**. La valeur par défaut est **12 000**.

Timeout Interval (Délai d'attente) : cette option définit la période d'attente au cours de laquelle l'agrégat doit être fermé avec une condition de clôture avant fermeture par la minuterie. Ce nombre peut être compris entre **0** et **100** ms. La valeur par défaut est **3**.

Min. Size of Packet in Aggregation (Taille minimum de paquet dans l'agrégation) : cette option définit la taille minimale (en octets) des paquets à cumuler dans l'agrégat. Ce nombre peut être compris entre **0** et **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai d'attente ADDBA) : cette option définit la durée au-delà de laquelle la configuration ADDBA est terminée, en l'absence d'échanges de trame dans ce délai par l'accord ACK (Block Acknowledgement, confirmation de bloc). Ce nombre peut être compris entre **0** et **65 535** ms. La valeur par défaut est **0**, ce qui désactive le délai d'attente.

Aggregation Window Size (Taille de la fenêtre d'agrégation) : cette option définit le nombre maximum de paquets transmis sans obtenir de confirmations. Ce nombre peut être compris entre **0** et **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Voice (Voix)

Use Aggregation (Utiliser l'agrégation) : cette option définit si la couche MAC (Media Access Control) configure une session ADDBA (Add Block Acknowledgement). La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Accept Aggregation (Accepter l'agrégation) : cette option définit si la couche MAC acceptera une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre maximum de paquets dans l'agrégation) : cette option définit le nombre maximum de paquets (sous-trames) dans l'agrégat. Ce nombre peut être compris entre **0** et **2**. La valeur par défaut est **2**.

Max. Aggregation Size (Taille maximale de l'agrégation) : cette option définit la taille maximale de l'agrégat (en octets). Ce nombre peut être compris entre **0** et **16 000**. La valeur par défaut est **10 000**.

Timeout Interval (Délai d'attente) : cette option définit la période d'attente au cours de laquelle l'agrégat doit être fermé avec une condition de clôture avant fermeture par la minuterie. Ce nombre peut être compris entre **0** et **100** ms. La valeur par défaut est **10**.

Min. Size of Packet in Aggregation (Taille minimum de paquet dans l'agrégation) : cette option définit la taille minimale (en octets) des paquets à cumuler dans l'agrégat. Ce nombre peut être compris entre **0** et **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai d'attente ADDBA) : cette option définit la durée au-delà de laquelle la configuration ADDBA est terminée, en l'absence d'échanges de trame dans ce délai par l'accord ACK (Block Acknowledgement, confirmation de bloc). Ce nombre peut être compris entre **0** et **65 535** ms. La valeur par défaut est **0**, ce qui désactive le délai d'attente.

Aggregation Window Size (Taille de la fenêtre d'agrégation) : cette option définit le nombre maximum de paquets transmis sans obtenir de confirmations. Ce nombre peut être compris entre **0** et **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Sans fil > Paramètres sans fil avancés

Configurez les fonctions sans fil avancées du pont. Il est préférable de réserver cette tâche à un administrateur chevronné, car des paramètres mal définis risqueraient de diminuer les performances de votre infrastructure sans fil.



REMARQUE
Les paramètres de l'écran *Advanced Wireless Settings* (Paramètres sans fil avancés) sont réservés aux utilisateurs avancés.

Paramètres sans fil avancés

Use LDPC (Utiliser LDPC) : LDPC (Low-Density Parity-Check Code) active ou désactive la correction des erreurs afin de réduire la probabilité de perte de données sur les canaux perturbés. L'algorithme d'adaptation du débit désactive automatiquement le codage LDPC lors de l'utilisation de débits PHY élevés (supérieurs à 162). Pour utiliser le système de correction d'erreur avancé LDCP, conservez la valeur par défaut **Yes** (Oui). Sinon, sélectionnez **No** (Non).

ERP Protection Type (Type de protection ERP) : cette option configure la protection des paquets OFDM malgré la présence de stations 802.11b dans le réseau sans fil. En envoyant des paquets RTS/CTS ou CTS2Self en débits 802.11b, le pont informe le réseau sans fil que des paquets OFDM vont être transférés et protège les paquets dans le réseau sans fil. Les paquets RTS/CTS et CTS2Self créent une surcharge, ce qui peut générer des débits plus faibles.

L'option RTS/CTS offre une meilleure couverture mais des débits inférieurs en comparaison avec CTS2Self, car l'option RTS/CTS inclut une confirmation du périphérique de réception. Pour utiliser l'option RTS/CTS, conservez la valeur par défaut **RTS/CTS**. L'option None (Aucune) peut entraîner des collisions entre les paquets OFDM et CCK. Pour utiliser cette option, sélectionnez **None** (Aucune). Pour utiliser l'option CTS2Self, sélectionnez **CTS2Self**.

11n Protection Type (Type de protection 11n) : cette option configure la protection de périphériques non haut débit dans le réseau sans fil. Dans le cas où le routeur sans fil (ou point d'accès) détecte une association de périphérique actuel non haut débit, il signale tous les périphériques haut débit pour utiliser les mécanismes RTS/CTS ou CTS2Self avant chaque transmission de données. Cette fonction prend également en charge toutes les protections de la norme 802.11n, y compris MIMO.

L'option RTS/CTS offre une meilleure couverture mais des débits inférieurs en comparaison avec CTS2Self, car l'option RTS/CTS inclut une confirmation du périphérique de réception. Pour utiliser l'option RTS/CTS, conservez la valeur par défaut **RTS/CTS**. L'option None (Aucune) peut entraîner des collisions entre les paquets haut débit et actuels. Pour utiliser cette option, sélectionnez **None** (Aucune). Pour utiliser l'option CTS2Self, sélectionnez **CTS2Self**.

Percentage of maximal transmit power (Pourcentage de puissance de transmission maximale) : cette option définit le pourcentage de puissance de transmission maximale par rapport aux restrictions du domaine de réglementation. Par exemple, si la restriction du domaine de réglementation autorise des transmissions jusqu'à 20 dB, la définition du pourcentage sur 50 % autorise une puissance de transmission maximale de 10 dB. Sélectionnez le pourcentage de votre choix : **12 %**, **25 %**, **50 %** ou **100 %**. La valeur par défaut est **100 %**.

QoS Classification Type (Type de classification QS) : cette option définit le mappage 802.1D ou 802.1Q à partir du champ IP DSCP/TOS sur des priorités WMM (Background (Arrière-plan), Best Effort (Effort maximum), Video (Vidéo), Voice (Voix)). Conservez la valeur par défaut **802.1D**, ou sélectionnez **802.1Q**, qui est utilisé par certains flux IPTV.

Re-establish Ethernet connection when initiating wireless connection (Rétablir la connexion Ethernet lors de l'activation de la connexion sans fil) : pour activer la découverte du protocole DHCP à partir du périphérique qui réside derrière le pont, le pont réinitialise la liaison Ethernet qui le relie avec le périphérique, à chaque fois qu'une connexion sans fil est établie. Pour désactiver cette fonction, sélectionnez **No** (Non). Sinon, conservez l'option par défaut **Yes** (Oui).

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Administration > Gestion

Utilisez cet écran pour gérer des fonctions de pont spécifiques : accès à l'utilitaire Web, sauvegarde du fichier de configuration, et redémarrage.



Gestion

Accès au pont

Utilisez un mot de passe pour protéger l'accès à l'utilitaire basé sur le navigateur Web.

Bridge Password (Mot de passe du pont) : saisissez un nouveau mot de passe pour le pont.

Re-enter to confirm (Confirmation du mot de passe) : saisissez à nouveau le mot de passe pour le confirmer.

Idle Timeout (Délai d'inactivité) : la connexion expire après une période d'inactivité que vous spécifiez. Ce délai peut être compris entre **60** et **3 600** secondes. La valeur par défaut est **600**.

Web Access (Accès Web)

Access via Wireless (Accès sans fil) : si vous utilisez votre pont dans un domaine public où vous offrez un accès sans fil à vos hôtes, vous pouvez désactiver l'accès sans fil à l'utilitaire basé sur le navigateur Web du pont. En désactivant ce paramètre, vous ne pourrez accéder à l'utilitaire basé sur le navigateur Web uniquement par une connexion câblée. Conservez le paramètre par défaut **Enabled** (Activé), pour autoriser l'accès sans fil à l'utilitaire basé sur le navigateur Web du pont, ou sélectionnez **Disabled** (Désactivé) pour le bloquer.

Backup and Restore (Sauvegarde et restauration)

Backup (Sauvegarde) : pour sauvegarder le fichier de configuration du pont, cliquez sur **Backup Configurations** (Sauvegarder les configurations). Suivez les instructions affichées à l'écran.

Restore (Restauration) : cliquez sur **Browse** (Parcourir) et sélectionnez le fichier de configuration. Cliquez ensuite sur **Restore Configurations** (Restaurer les configurations).

Redémarrage système

Reboot (Redémarrage) : pour redémarrer ou relancer le pont, cliquez sur **Start to Reboot** (Lancer le redémarrage).

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Administration > Paramètres d'usine

Utilisez cet écran pour restaurer la configuration du pont sur ses paramètres par défaut d'usine.

Paramètres d'usine

Restore All Settings (Restaurer tous les paramètres) : pour rétablir les paramètres par défaut d'usine du pont, cliquez sur **Restore All Settings** (Restaurer tous les paramètres). Tous les paramètres enregistrés précédemment seront perdus une fois les paramètres par défaut restaurés.



Administration > Mise à niveau du micrologiciel

Utilisez cet écran pour mettre à niveau le micrologiciel du pont. Ne mettez pas à niveau votre micrologiciel sauf si vous rencontrez des problèmes avec le pont ou si la nouvelle version du micrologiciel offre une fonctionnalité que vous souhaitez utiliser.



Avant de mettre à niveau le micrologiciel, téléchargez le fichier de mise à niveau du micrologiciel du pont depuis le site Web de Linksys **www.Linksys.com/support**.

Mise à niveau du micrologiciel

Please select a file to upgrade the firmware (Sélectionnez un fichier pour la mise à niveau du micrologiciel) : cliquez sur **Browse** (Parcourir) et sélectionnez le fichier de mise à niveau du micrologiciel. Cliquez ensuite sur **Start to Upgrade** (Lancer la mise à niveau) et suivez les instructions à l'écran.

Etat > Pont

Les informations d'état actuel du pont sont affichées.



Informations concernant le pont

Firmware Version (Version du micrologiciel) : identifie le micrologiciel actuel du pont.

Réseau local

Local MAC Address (Adresse MAC locale) : indique l'adresse MAC du pont, telle qu'elle apparaît sur votre réseau Ethernet local.

IP Address (Adresse IP) : indique l'adresse IP du pont, telle qu'elle apparaît sur votre réseau Ethernet local.

Subnet Mask (Masque de sous-réseau) : indique le masque de sous-réseau configuré pour votre réseau local.

Etat > Sans fil

Les informations sur votre réseau sans fil sont affichées.



Sans fil

Link Status (Etat de la liaison) : indique l'état de la connexion avec votre réseau sans fil.

MAC Address (Adresse MAC) : indique l'adresse MAC du pont, telle qu'elle apparaît sur votre réseau sans fil local.

Network Name (SSID) (Nom du réseau (SSID)) : indique le nom du réseau sans fil ou SSID.

BSSID : indique l'adresse MAC sans fil du routeur sans fil connecté (ou point d'accès).

Radio Band (Bande radio) : indique la bande radio de votre réseau sans fil.

Channel Width (Largeur du canal) : indique la largeur du canal, en MHz, utilisé par votre réseau sans fil.

Wide Channel (Canal à large bande) : indique le canal à large bande, selon les paramètres de canal de votre routeur réseau. Si vous avez sélectionné Wide - 40MHz Channel (Large bande - Canal 40 MHz) comme paramètre de bande radio ou de largeur du canal du routeur, il s'agira de votre canal sans fil N principal.

Standard Channel (Canal standard) : indique le paramètre de canal standard. Si vous avez sélectionné Wide – 40MHz Channel (Large bande - Canal 40 MHz) comme paramètre de bande radio ou de largeur du canal du routeur, le canal standard servira de canal auxiliaire pour les connexions sans fil N.

Bit Rate (Nombre de bits) : indique le taux de transmission des données.

Signal : correspond au pourcentage d'intensité du signal. 100 % indique l'intensité maximale ; 0 % identifie le niveau le plus faible.

Security (Sécurité) : indique la méthode de sécurité de votre réseau sans fil.

Dépannage

WES610N/WET610N

Votre ordinateur ou un autre périphérique Ethernet câblé ne peut pas communiquer avec le routeur sans fil.

1. Accédez à l'utilitaire basé sur le navigateur Web du pont.
2. Dans l'écran *Basic Wireless Settings* (Paramètres sans fil de base), vérifiez que le nom du réseau (SSID) correspond au nom de votre réseau sans fil.
3. Assurez-vous que les paramètres de sécurité (WPA, WPA2 ou WEP) correspondent à ceux de votre réseau sans fil.

L'adresse IP du pont doit être modifiée.

Si le pont est connecté à un réseau avec un serveur DHCP (généralement le routeur réseau), il obtient son adresse IP auprès du serveur DHCP. En l'absence de serveur DHCP, le pont utilise son adresse IP statique par défaut, **169.254.1.250**.

Pour que le pont utilise toujours une adresse IP statique, suivez ces instructions :

1. Accédez à l'utilitaire basé sur le navigateur Web du pont.
2. Cliquez sur l'onglet **Network Setup** (Configuration réseau).
3. Dans le menu déroulant *Network Connection Type* (Type de connexion réseau), sélectionnez **Static IP** (Adresse IP statique).
4. Complétez les champs *Static IP Address* (Adresse IP statique), *Subnet Mask* (Masque de sous-réseau) et *Default Gateway* (Passerelle par défaut).
5. Cliquez sur **Save Settings** (Enregistrer les paramètres).

L'ordinateur activé par le pont ou un autre périphérique Ethernet câblé n'arrive pas à communiquer avec un autre périphérique compatible sans fil (comme un ordinateur ou une imprimante).

Vérifiez les points suivants :

- Assurez-vous que le périphérique compatible sans fil se trouve sur le même réseau sans fil que l'ordinateur ou l'autre périphérique Ethernet câblé relié au pont.
- Vérifiez que le même nom de réseau (SSID) est utilisé pour tous les périphériques du réseau sans fil.
- Assurez-vous que tous les périphériques se trouvent sur le même réseau IP et utilisent des adresses IP compatibles.

L'utilitaire basé sur le navigateur Web n'accepte pas votre mot de passe.

Vérifiez les points suivants :

- Le mot de passe est sensible à la casse. Veillez à utiliser la casse qui convient lors de la saisie du mot de passe.
- Si vous avez oublié votre mot de passe, vous pouvez rétablir les paramètres par défaut d'usine du pont.

 Maintenez le bouton **Reset** (Réinitialisation) du pont enfoncé pendant environ cinq secondes ; le mot de passe est rétabli sur sa valeur par défaut d'usine, **admin**. Tous les autres paramètres du pont reviennent également aux valeurs par défaut d'usine. (Pour accéder à l'utilitaire basé sur le navigateur Web, saisissez **admin** dans le champ *Password* (Mot de passe).)

Une fois les modifications apportées via l'utilitaire basé sur le navigateur Web, les nouveaux paramètres n'apparaissent pas à l'écran.

Actualisez votre navigateur Web. Si les nouveaux paramètres ne s'affichent pas, suivez ces instructions :

1. Débranchez l'adaptateur électrique du pont.
2. Attendez cinq secondes, puis rebranchez l'adaptateur sur le pont.
3. **Actualisez** votre navigateur Web.

WEB
Si certaines de vos questions ne sont pas abordées dans cette annexe, consultez le site Web de Linksys à l'adresse suivante : **Linksys.com/support**.

Spécifications

WES610N

Modèle	WES610N
Normes	IEEE 802.3u, 802.11g, 802.11b, 802.11a et 802.11n
Voyants	Alimentation, Ethernet, Wi-Fi Protected Setup™, Sans fil, activité et liaison Ethernet individuelles
Ports	Ethernet (4), Alimentation
Boutons	Reset (Réinitialisation), Wi-Fi Protected Setup
Type de câblage	CAT5e
Antennes	3 (internes)
Type de connecteur d'antenne	N/A
Amovible (Oui/Non)	Non
Modulations	802.11a : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b : CCK/QPSK, BPSK 802.11g : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n : OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Puissance RF (EIRP) en dBm	802.11a : 15 dBm (utilisation normale) à 54 Mbit/s 802.11b : 19 dBm (utilisation normale) à 11 Mbit/s 802.11g : 16 dBm (utilisation normale) à 54 Mbit/s 802.11n (2,4 GHz) : 18 dBm (utilisation normale) à MCS15 802.11n (5 GHz) : 16 dBm (utilisation normale) à MCS15
Sensibilité en réception	802.11a : -72 dBm (utilisation normale) à 54 Mbit/s 802.11b : -85 dBm (utilisation normale) à 11 Mbit/s 802.11g : -73 dBm (utilisation normale) à 54 Mbit/s 802.11n (20 MHz) : -75 dBm (utilisation normale) à MCS15 802.11n (40 MHz) : -69 dBm (utilisation normale) à MCS15
Gain de l'antenne en dBi	1
Sécurité sans fil	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Configuration binaire de la clé de sécurité	Cryptage jusqu'à 128 bits

Conditions environnementales

Dimensions :	177 x 128 x 68 mm
Poids	295 g
Certification	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802.11a/b/g/pré-standard n), WPA2™, Wi-Fi Protected Setup™, WMM®
Alimentation	12 V, 1 A
Température de fonctionnement	de 0 à 40 °C
Température de stockage	de -20 à 60 °C
Humidité en fonctionnement	10 à 85 %, non condensée
Humidité de stockage	5 à 90 %, non condensée

Les spécifications peuvent être modifiées sans préavis.

WET610N

Modèle	WET610N
Normes	IEEE 802.3u, 802.11g, 802.11b, 802.11a et 802.11n
Voyants	Alimentation, Ethernet, Wi-Fi Protected Setup™, Sans fil
Ports	Ethernet, Power (Alimentation)
Boutons	Reset (Réinitialisation), Wi-Fi Protected Setup
Type de câblage	CAT5e
Antennes	3 (internes)
Type de connecteur d'antenne	N/A
Amovible (Oui/Non)	Non
Modulations	802.11a : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b : CCK/QPSK, BPSK 802.11g : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n : OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Puissance RF (EIRP) en dBm	802.11a : 15 dBm (utilisation normale) à 54 Mbit/s 802.11b : 18 dBm (utilisation normale) à 11 Mbit/s 802.11g : 16 dBm (utilisation normale) à 54 Mbit/s 802.11n : 12 dBm (utilisation normale) à 130 Mbit/s (HT20), 270 Mbit/s (HT40)
Sensibilité en réception	802.11a : -72 dBm (utilisation normale) à 54 Mbit/s 802.11b : -85 dBm (utilisation normale) à 11 Mbit/s 802.11g : -73 dBm (utilisation normale) à 54 Mbit/s 802.11n : -70 dBm (utilisation normale) à MCS15/2,4 GHz, -69 dBm (utilisation normale) à MCS15/5,0 GHz
Gain de l'antenne en dBi	1
Sécurité sans fil	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Configuration binaire de la clé de sécurité	Cryptage jusqu'à 128 bits

Conditions environnementales

Dimensions	145 x 106 x 52 mm
Poids	159 g
Certification	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802.11a/b/g/pré-standard n), WPA2™, Wi-Fi Protected Setup™, WMM®
Alimentation	12 V, 1 A
Température de fonctionnement	de 0 à 40 °C
Température de stockage	de -20 à 60 °C
Humidité en fonctionnement	10 à 85 %, non condensée
Humidité de stockage	5 à 90 %, non condensée

Les spécifications peuvent être modifiées sans préavis.

Linksys.com/support

Cisco, le logo Cisco et Linksys sont des marques commerciales ou déposées de Cisco et/ou de ses filiales aux Etats-Unis et dans d'autres pays.
La liste des marques commerciales de Cisco est disponible sur www.cisco.com/go/trademarks. Toutes les autres marques commerciales mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs.

© 2011, Cisco et/ou ses filiales. Tous droits réservés.

3425-01249



Guide de l'utilisateur

Linksys WET610N/WES610N | Pont sans fil N double bande

Table des matières

Vue d'ensemble du produit

Panneau de voyants 2
Panneau des ports 3

Conseils pour accroître la sécurité de votre réseau sans fil

Changer le nom de réseau sans fil par défaut (SSID) 4
Changer le mot de passe par défaut 4
Activer le filtrage d'adresses MAC 4
Activer le cryptage 4

Directives générales de sécurité de réseau 4
Autres conseils de sécurité 5

Configuration avancée

Accès à l'utilitaire Web 6
Setup (Configuration) > Basic Setup (Configuration de base) . . . 7
Language (Langue) 7
Network Setup (Configuration du réseau) 7

Wireless (Sans fil) > Basic Wireless Settings (Paramètres de base du réseau sans fil) 7
Paramètres de base du réseau sans fil 8
Sécurité sans fil 8
Configuration de l'accès Wi-Fi protégé 9

Wireless (Sans fil) > Wireless Network Site Survey (Analyse du réseau sans fil) 10
Wireless Network Site Survey (Analyse du réseau sans fil) 10

Wireless (Sans fil) > WMM® 11
WMM 12

Wireless (Sans fil) > Advanced Wireless Settings (Paramètres sans fil avancés) 13
Advanced Wireless (Paramètres sans fil avancés) 14

Administration > Management (Gestion) 14
Management (Gestion) 14

Administration > Factory Defaults (Paramètres par défaut d'usine) 15
Factory Defaults (Paramètres par défaut d'usine) 15

Administration > Upgrade Firmware (Mise à niveau du microcode) 15
Upgrade Firmware (Mise à niveau du microcode) 15

Status (État) > Bridge (Pont) 15
Bridge Information (Informations sur le pont) 16
Local Network (Réseau local) 16

Status (État) > Wireless (Sans fil) 16
Wireless (Sans fil) 16

Dépannage

WES610N/WET610N 17

Spécifications

WES610N 18
WET610N 19

Vue d'ensemble du produit

Merci d'avoir choisi le pont sans fil N à double bande de Linksys. Le pont peut connecter n'importe quel dispositif Ethernet câblé à votre réseau sans fil. Le pont est basé sur la technologie sans fil N double bande, donc il est compatible avec tous les routeurs sans fil N, G, A ou B ou points d'accès. Pour une installation initiale, effectuez les étapes indiquées dans le dossier du CD. Pour configurer les paramètres avancés, servez-vous de l'utilitaire Web.

Panneau de voyants



WES610N WET610N

Sans fil (bleu) Ce voyant s'allume pour indiquer qu'une connexion sans fil est établie. Le voyant clignote lorsque le pont envoie ou reçoit des données sur le réseau sans fil.

Bouton de configuration d'accès Wi-Fi protégé Si votre routeur prend en charge la configuration Wi-Fi protégée et utilise la sécurité WPA ou WPA2, alors vous pouvez utiliser Wi-Fi Protected Setup pour connecter automatiquement le pont. Pour utiliser la configuration d'accès Wi-Fi protégé, consultez « Wireless (Sans fil) > Basic Wireless Settings (Paramètres de base du réseau sans fil) » à la page 7.

Voyant de configuration d'accès Wi-Fi protégé (bleu/ambre) Ce voyant clignote en bleu durant deux minutes pendant la configuration de l'accès Wi-Fi protégé. Il demeure allumé en bleu une fois la sécurité sans fil activée. Si une erreur survient durant la configuration de l'accès Wi-Fi protégé, alors le voyant devient ambre. Assurez-vous que le routeur prend en charge la configuration d'accès Wi-Fi protégé. Attendez que le voyant soit éteint, puis recommencez.

Ethernet (bleu) Le voyant Ethernet s'allume lorsqu'une connexion Ethernet est établie. Le voyant clignote quand le pont envoie ou reçoit des données sur un port Ethernet.

Alimentation (bleu) Le voyant d'alimentation s'allume quand le pont est sous tension.

Panneau des ports



WES610N WET610N

Ethernet Les ports Ethernet servent à connecter le pont à un ordinateur ou à un autre périphérique réseau Ethernet. Le pont WES610N comporte quatre ports et le WET610N en comporte un seul.

Reset (Réinitialiser) Il existe deux façons de restaurer les paramètres par défaut du pont. Maintenez enfoncé le bouton Reset pendant environ cinq secondes, ou utilisez l'option Administration > Valeurs par défaut de l'utilitaire Web du pont. Le bouton de réinitialisation se trouve sous le boîtier du pont WES610N, tandis que celui du WET610N se trouve sur le panneau des ports à l'arrière.

Power (Alimentation) Le port d'alimentation permet de brancher l'adaptateur de courant fourni.

Conseils pour accroître la sécurité de votre réseau sans fil

Les réseaux sans fil étant pratiques et faciles à installer, ils sont de plus en plus populaires auprès des ménages dotés d'un accès Internet haute vitesse. Cependant, puisque les réseaux sans fil transmettent les données par ondes radios, ils peuvent être plus vulnérables aux intrus qu'un réseau Ethernet. À l'instar des signaux transmis par téléphones cellulaires ou sans fil, ceux d'un réseau sans fil peuvent également être interceptés. Puisque vous ne pouvez pas empêcher physiquement les intrus de se connecter à votre réseau sans fil, vous devez prendre des mesures supplémentaires pour le sécuriser.

Changer le nom de réseau sans fil par défaut (SSID)

Les appareils sans fil ont un nom de réseau sans fil par défaut ou « Service Set Identifier » (SSID) établi par le fabricant. Il constitue le nom de votre réseau sans fil et peut contenir jusqu'à 32 caractères. Les produits sans fil Linksys utilisent **linksys** comme nom de réseau sans fil par défaut. Nous vous suggérons de donner un nom exclusif à votre réseau sans fil afin de le distinguer des autres réseaux sans fil à proximité. Cependant, ne vous inspirez pas de renseignements personnels (par exemple, votre numéro d'assurance sociale) pour choisir ce nom, car n'importe qui pourrait accéder à cette information en accédant à votre réseau.

Changer le mot de passe par défaut

Pour les périphériques sans fil comme les points d'accès et les routeurs, vous devrez entrer un mot de passe pour changer leurs paramètres. Ces appareils ont un mot de passe par défaut établi par le fabricant. Le mot de passe par défaut de Linksys est **admin**. Tous les pirates connaissent ces valeurs par défaut et pourraient les utiliser pour accéder à votre périphérique sans fil et changer vos paramètres de réseau. Pour empêcher ces changements non autorisés, choisissez un mot de passe difficile à deviner.

Activer le filtrage d'adresses MAC

Les routeurs Linksys vous permettent d'utiliser le filtrage d'adresse MAC (Media Access Control). L'adresse MAC est une suite de caractères alphanumériques attribuée à tous les périphériques du réseau. Lorsque le filtrage d'adresse MAC est activé, l'accès au réseau sans fil est fourni exclusivement aux périphériques dotés d'adresses MAC spécifiques. Par exemple, vous pouvez entrer une adresse MAC pour chaque ordinateur de la maison afin que seuls ces ordinateurs puissent accéder à votre réseau sans fil.

Activer le cryptage

Le cryptage protège les données qui sont transmises sur un réseau sans fil. Les modes de cryptage Wi-Fi Protected Access (WPA/WPA2) et Wired Equivalency Privacy (WEP) offrent différents niveaux de sécurité pour les transmissions sans fil.

WPA/WPA2 faisant appel au cryptage par clé dynamique, il est plus sûr que le mode WEP. Pour protéger les données transmises par radio, activez le plus haut niveau de cryptage que votre matériel réseau peut prendre en charge.

Le cryptage WEP étant moins récent, c'est parfois la seule option offerte pour les périphériques non compatibles avec WPA.

Directives générales de sécurité de réseau

La sécurité d'un réseau sans fil est inutile si le réseau sous-jacent n'est pas sécurisé.

- Vous devez protéger par mot de passe les ordinateurs et les fichiers critiques du réseau.
- Changez vos mots de passe régulièrement.
- Installez un antivirus et un pare-feu.
- Désactivez le partage de fichiers d'égal à égal (P2P). Certaines applications activent parfois le partage de fichiers à votre insu.

Autres conseils de sécurité

- Éloignez les routeurs, points d'accès et passerelles sans fil des murs extérieurs et des fenêtres.
- Éteignez les routeurs, points d'accès et passerelles sans fil lorsqu'ils ne sont pas utilisés (durant la nuit ou pendant les vacances, par exemple).
- Utilisez des phrases de vérification fortes contenant au moins huit caractères. Combinez des lettres et des chiffres pour éviter d'utiliser des mots qui peuvent être trouvés dans un dictionnaire.

Configuration avancée

Une fois le pont configuré en suivant les étapes indiquées dans le dossier du CD, il sera prêt à être utilisé. Toutefois, si vous désirez modifier ses paramètres avancés, utilisez l'utilitaire Web du pont. Le présent chapitre explique chaque page Web de l'utilitaire et les principales options proposées sur chacune. Vous pouvez accéder à l'utilitaire depuis un navigateur Web sur un ordinateur connecté au réseau du pont.

L'utilitaire Web présente les onglets principaux suivants : Setup (Configuration), Wireless (Sans fil), Administration et Status (État). D'autres onglets sont accessibles à partir des onglets principaux.

Accès à l'utilitaire Web

Utilisez un navigateur Web pour accéder à l'utilitaire Web.

Si le pont est connecté à un réseau doté d'un serveur DHCP (il s'agit généralement d'un routeur), alors le serveur DHCP fournira une adresse IP au pont. Si aucun serveur DHCP n'est disponible, alors le pont utilisera son adresse IP statique par défaut, soit **169.254.1.250**. (Si vous avez affecté une adresse IP statique permanente au pont à l'aide de l'utilitaire Web, alors entrez plutôt cette adresse.)

REMARQUE
Si vous ne savez pas quelle est l'adresse IP est attribuée au pont, alors recherchez-la dans la table des clients DHCP du routeur. (Reportez-vous à la documentation de votre routeur.)

Si vous n'arrivez pas à identifier l'adresse IP de votre pont, vous pouvez le réinitialiser. Appuyez sur le bouton **Reset** (Réinitialisation) sur le pont pendant environ cinq secondes, à l'aide d'un trombone déplié. Cela aura pour effet de réinitialiser le pont et d'y rétablir les paramètres par défaut. Le pont demandera une adresse IP au serveur DHCP (qui est généralement le routeur). Si aucun serveur DHCP n'est détecté, alors le pont utilisera son adresse IP par défaut, soit **169.254.1.250**, jusqu'à ce qu'un serveur DHCP soit détecté et que celui-ci lui ait attribué une adresse IP dynamique.

Si le pont n'est pas associé à un routeur et qu'il utilise les paramètres par défaut, connectez un ordinateur au pont à l'aide d'une connexion Ethernet, pour accéder à l'utilitaire -Web. Vous devrez configurer la connexion Ethernet de l'ordinateur en y définissant une adresse IP statique et un masque de sous-réseau.

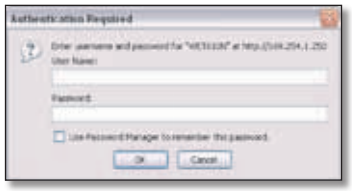
L'adresse IP de votre adaptateur Ethernet devrait être définie de manière précise.

1. Dans le champ *IP address* (Adresse IP), entrez **169.254.x.y** (où x représente un nombre entre 1 et 254, et y représente un nombre entre 0 et 255).
2. Dans le champ *Subnet mask* (Masque de sous-réseau), entrez **255.255.0.0**.

REMARQUE
Les étapes permettant d'attribuer une adresse IP statique à l'adaptateur Ethernet de votre ordinateur dépendent de votre système d'exploitation. Pour obtenir des instructions, veuillez vous référer à la documentation de votre système d'exploitation.

Après avoir attribué une adresse IP statique à votre adaptateur Ethernet, lancez votre navigateur Web et entrez l'adresse IP par défaut de l'adaptateur (la valeur par défaut est **169.254.1.250**) dans le champ *Address* (Adresse). Appuyez sur **Entrée**.

Une boîte de dialogue s'affiche, vous demandant un mot de passe. (Une fenêtre similaire s'affiche sur les systèmes autres que Windows XP.) N'entrez rien dans le champ *User Name* (Nom d'utilisateur). Entrez le mot de passe que vous avez créé dans l'assistant d'installation. Si vous n'avez pas créé de mot de passe, utilisez le mot de passe par défaut, soit **admin**. (Vous pouvez choisir un nouveau mot de passe à partir de l'écran *Administration* > *Management* (Gestion).) Cliquez sur **OK** pour continuer.



REMARQUE
Si la demande de mot de passe ne s'affiche pas, attendez deux minutes et essayez de nouveau.

Setup (Configuration) > Basic Setup (Configuration de base)

Le premier écran qui apparaît est *Basic Setup* (Configuration de base). Utilisez cet écran pour changer la langue de l'utilitaire Web ou modifier les réglages du réseau Ethernet câblé du pont.





Language (Langue)

Langage (Langue) Permet de choisir la langue de l'utilitaire Web. Sélectionnez la langue voulue dans le menu déroulant.

Network Setup (Configuration du réseau)

Cette section détermine si l'adresse IP du pont est obtenue automatiquement d'un serveur DHCP, comme votre routeur (Automatic Configuration (Configuration automatique) - DHCP) ou réglée manuellement (Static IP (Adresse IP statique)).

Bridge IP (Adresse IP du pont) Si votre réseau comporte un serveur DHCP, comme par exemple votre routeur, qui attribue des adresses IP aux périphériques, alors conservez la valeur par défaut, **Automatic Configuration** (Configuration automatique) **- DHCP**. Le pont demandera une adresse IP au serveur DHCP (qui est généralement le routeur). Si aucun serveur DHCP n'est détecté, alors le pont utilisera son adresse IP par défaut, soit **169.254.1.250**, jusqu'à ce qu'un serveur DHCP soit détecté et que celui-ci lui ait attribué une adresse IP dynamique.

Si vous voulez définir une adresse IP statique permanente pour le pont, sélectionnez **Static IP** (Adresse IP statique).

Si vous sélectionnez cette option, alors vous devrez remplir les champs suivants :

- **Static IP Address** (Adresse IP statique) Entrez une adresse IP unique, que vous utiliserez pour accéder à l'utilitaire Web.
- **Subnet Mask** (Masque de sous-réseau) Entrez le masque de sous-réseau de votre réseau Ethernet.
- **Default Gateway** (Passerelle par défaut) Entrez l'adresse IP de la passerelle par défaut de votre réseau (dans la plupart des cas, il s'agit de votre routeur).

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Wireless (Sans fil) > Basic Wireless Settings (Paramètres de base du réseau sans fil)

Utilisez l'écran *Basic Wireless Settings* (Paramètres de base du réseau sans fil) pour configurer les paramètres sans fil et de sécurité du pont.

Le pont peut être configuré de deux façons, soit manuellement ou avec la configuration de l'accès Wi-Fi protégé. La configuration de l'accès Wi-Fi protégé facilite la configuration de votre réseau sans fil. Si votre routeur prend en charge la configuration de l'accès Wi-Fi protégé et utilise la sécurité WPA ou WPA2, alors vous pouvez utiliser la configuration de l'accès Wi--Fi protégé pour connecter le pont automatiquement.

Configuration View (Vue de configuration) Pour configurer votre réseau sans fil manuellement, sélectionnez **Manual** (Manuelle). Reportez-vous à la section **Paramètres de base du réseau sans fil**, **page 8**. Pour utiliser la configuration de l'accès Wi-Fi protégé, sélectionnez **Wi-Fi Protected Setup** (Configuration de l'accès Wi-Fi protégé). Reportez-vous à la section **Configuration de l'accès Wi-Fi protégé**, **page 9**.

Paramètres de base du réseau sans fil



Network Name (SSID) (Nom de réseau - SSID) Le SSID est le nom de réseau que partagent tous les points d'un réseau sans fil. Ce nom doit être identique pour tous les périphériques du réseau. Le système distingue les minuscules et les majuscules, et le nom ne doit pas compter plus de 32 caractères (tous les caractères du clavier sont acceptés). Assurez-vous que ce réglage correspond au réglage de votre routeur sans fil ou de votre point d'accès. Pour plus de sécurité, remplacez le SSID par défaut (**linksys**).

Sécurité sans fil

Le pont prend en charge les options de sécurité sans fil suivantes : WPA Personal, WPA2 Personal et WEP. Les méthodes de sécurité WPA (Wi-Fi Protected Access, ou accès protégé sans fil) et WPA2 sont plus puissantes que WEP (Wired Equivalent Privacy, ou confidentialité sans fil équivalente à celle d'un réseau Ethernet). Pour de plus amples renseignements sur la sécurité sans fil, reportez-vous à la section « Conseils pour accroître la sécurité de votre réseau sans fil », page 4.

Security Mode (Mode de sécurité)

Sélectionnez le mode de sécurité utilisé par votre réseau sans fil. Si vous ne voulez pas sécuriser votre réseau sans fil, conservez la valeur par défaut, soit **Disabled** (Désactivé).

REMARQUE
N'oubliez pas que chaque appareil de votre réseau sans fil DOIT utiliser la même méthode de sécurité et la même phrase de vérification ou clé, sans quoi les appareils sans fil ne seront pas en mesure de communiquer entre eux.

WPA Personal (WPA personnel)

WPA est une norme de sécurité plus robuste que le cryptage WEP.



Encryption (Cryptage) Le mode WPA prend en charge la méthode de cryptage TKIP, avec le cryptage dynamique des clés.

Passphrase (Phrase de vérification) Entrez la clé partagée par le pont et par votre routeur sans fil ou point d'accès. Cette clé doit comporter de 8 à 63 caractères.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

WPA2 Personal (WPA2 personnel)

WPA2 est une version plus sécuritaire et plus évoluée de la norme WPA.



Encryption (Cryptage) Le mode WPA2 prend en charge deux modes de cryptage avec clés dynamiques, soit TKIP et AES. Sélectionnez un mode de cryptage, soit **AES**, **TKIP ou AES**. La sélection par défaut est **AES**.

Passphrase (Phrase de vérification) Entrez la clé partagée par le pont et par votre routeur sans fil ou point d'accès. Cette clé doit comporter de 8 à 63 caractères.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

WEP

WEP est un mode de cryptage de base moins sûr que WPA ou WPA2.



Encryption (Cryptage) Sélectionnez le niveau de cryptage WEP voulu**, soit 40/64 bits (10 caractères hexadécimaux)** ou **104/128 bits (26 caractères hexadécimaux)**. Le paramètre par défaut est **40/64 bits (10 caractères hexadécimaux)**.

Key 1 (Clé 1) Entrez la clé WEP de votre réseau.

Tx Key (Clé de transmission) **Key 1** (Clé 1) est la clé de transmission utilisée par le pont.

Authentication (Authentification) La valeur par défaut est **Auto**, ce qui autorise l'authentification Système ouvert ou Clé partagée. Sélectionnez **Open** (Ouvert) pour utiliser l'authentification Système ouvert; l'expéditeur et le destinataire n'utilisent pas une clé WEP pour l'authentification. Sélectionnez **Shared** (Partagée) pour utiliser l'authentification par clé partagée; l'expéditeur et le destinataire utilisent une clé WEP pour l'authentification.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Configuration de l'accès Wi-Fi protégé

Deux méthodes peuvent être utilisées. Utilisez la méthode qui s'applique au routeur que vous configurez.





Méthode 1

Utilisez cette méthode si votre routeur est doté d'une touche Wi-Fi Protected Setup (Configuration de l'accès Wi-Fi protégé).

1. Appuyez sur la touche **Wi-Fi Protected Setup** (Configuration de l'accès Wi-Fi protégé) du routeur.
2. Dans les deux minutes qui suivent, cliquez sur le bouton **Wi-Fi Protected Setup** (Configuration de l'accès Wi-Fi protégé) sur l'écran *Wi-Fi Protected Setup* du pont.
3. Après la configuration du pont, cliquez sur **Close** (Fermer).

L'écran *Wi-Fi Protected Setup* (configuration de l'accès Wi-Fi protégé) affiche les champs suivants : Link Status (état du lien), Network Name (nom du réseau - SSID) et Security method (méthode de sécurité).

Méthode 2

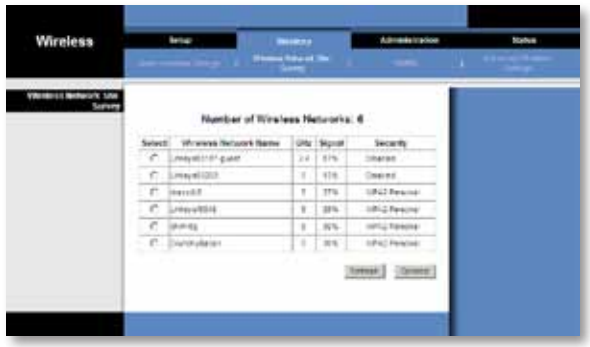
Utilisez cette méthode si votre routeur demande le NIP du pont.

1. À l'écran *Wi-Fi Protected Setup* (Configuration de l'accès Wi-Fi protégé) du **routeur**, entrez le NIP à l'écran *Wi-Fi Protected Setup* du **pont**. Ensuite, cliquez sur **Register** (Enregistrer) ou sur le bouton approprié. (Le NIP est également inscrit sur une étiquette apposée sous le pont).
2. À l'écran *Wi-Fi Protected Setup* (Configuration de l'accès Wi-Fi protégé) du **pont**, cliquez sur **OK**.
3. Après la configuration du pont, cliquez sur **Close** (Fermer).

L'écran *Wi-Fi Protected Setup* (Configuration de l'accès Wi-Fi protégé) affiche les champs suivants : Link Status (État du lien), Network Name (Nom du réseau - SSID) et Security method (Méthode de sécurité).

Wireless (Sans fil) > Wireless Network Site Survey (Analyse du réseau sans fil)

Cliquez sur l'onglet **Wireless Network Site Survey** (Analyse du réseau sans fil) pour débuter une analyse du site. L'écran *Wireless Network Site Survey* (Analyse du réseau sans fil) répertorie les réseaux sans fil détectés par le pont.



Wireless Network Site Survey (Analyse du réseau sans fil)

Number of Wireless Networks (Nombre de réseaux sans fil) Le nombre de réseaux sans fil détectés par le pont est affiché.

Select (Sélectionner) Pour se connecter à un réseau sans fil, cliquez sur **Select** (Sélectionner). Cliquez ensuite sur **Connect** (Connecter).

Wireless Network Name (Nom du réseau sans fil) Le nom du réseau sans fil ou le SSID du réseau sans fil est affiché.

GHz La bande radio du réseau sans fil est affichée.

Signal Le pourcentage de la puissance du signal est affiché. 100 % est la puissance de signal la plus forte et 0 % est la plus faible possible.

Security (Sécurité) Si le réseau prend en charge la configuration de l'accès Wi-Fi protégé, alors l'icône Wi-Fi Protected Setup (Configuration de l'accès Wi-Fi protégé) est affichée. La méthode de sécurité utilisée par le réseau sans fil est affichée.

Pour mettre à jour les renseignements de l'écran, cliquez sur **Refresh** (Actualiser).

Après avoir sélectionné un réseau, cliquez sur **Connect** (Connecter). Un nouvel écran apparaît. Suivez les instructions pour la méthode de sécurité de votre réseau.

WPA



Network Name (SSID) (Nom de réseau - SSID) Le nom de réseau que vous avez sélectionné s'affiche automatiquement.

Security Mode (Mode de sécurité) WPA Personal (WPA personnel) est automatiquement affiché.

Encryption (Cryptage) Le mode WPA prend en charge la méthode de cryptage TKIP, avec le cryptage dynamique des clés.

Passphrase (Phrase de vérification) Entrez la clé partagée par le pont et par votre routeur sans fil ou point d'accès. Cette clé doit comporter de 8 à 63 caractères.

Pour mettre à jour les renseignements de l'écran, cliquez sur **Refresh** (Actualiser).

Après avoir entré les paramètres de sécurité, cliquez sur **Connect** (Connecter).

WPA2



Network Name (SSID) (Nom de réseau - SSID) Le nom de réseau que vous avez sélectionné s'affiche automatiquement.

Security Mode (Mode de sécurité) WPA2 Personal (WPA2 personnel) est automatiquement affiché.

Encryption (Cryptage) Le mode WPA2 prend en charge deux modes de cryptage avec clés dynamiques, soit TKIP et AES. Sélectionnez un mode de cryptage, soit **AES**, **TKIP ou AES**.

Passphrase (Phrase de vérification) Entrez la clé partagée par le pont et par votre routeur sans fil ou point d'accès. Cette clé doit comporter de 8 à 63 caractères.

Pour mettre à jour les renseignements de l'écran, cliquez sur **Refresh** (Actualiser).

Après avoir entré les paramètres de sécurité, cliquez sur **Connect** (Connecter).

WEP



Network Name (SSID) (Nom de réseau - SSID) Le nom de réseau que vous avez sélectionné s'affiche automatiquement.

Security Mode (Mode de sécurité) WEP est automatiquement affiché.

Encryption (Cryptage) Sélectionnez le niveau de cryptage WEP voulu, soit **40/64 bits (10 caractères hexadécimaux)** ou **104/128 bits (26 caractères hexadécimaux)**.

Key 1 (Clé 1) Entrez la clé WEP de votre réseau.

Tx Key (Clé de transmission) **Key 1** (Clé 1) est la clé de transmission utilisée par le pont.

Authentication (Authentification) La valeur par défaut est **Auto**, ce qui autorise l'authentification Système ouvert ou Clé partagée. Sélectionnez **Open** (Ouvert) pour utiliser l'authentification Système ouvert; l'expéditeur et le destinataire n'utilisent pas une clé WEP pour l'authentification. Sélectionnez **Shared** (Partagée) pour utiliser l'authentification par clé partagée; l'expéditeur et le destinataire utilisent une clé WEP pour l'authentification.

Pour mettre à jour les renseignements de l'écran, cliquez sur **Refresh** (Actualiser).

Après avoir entré les paramètres de sécurité, cliquez sur **Connect** (Connecter).

Wireless (Sans fil) > WMM®

Configurez les paramètres WMM (Wireless MultiMedia, ou multimédia sans fil). WMM définit les priorités des paquets selon leur mode d'accès respectif (type de trafic) : Background (Arrière-plan), Best Effort (Meilleur effort), Video (Vidéo) ou Voice (Voix). La configuration devrait être confiée à un administrateur réseau car des paramètres incorrects peuvent réduire les performances des transmissions sans fil.



REMARQUE
Les paramètres de l'écran *WMM* sont conçus pour les utilisateurs avancés seulement.

WMM

Access Mode (Mode d'accès)

Vous pouvez attribuer des paramètres différents aux quatre modes d'accès disponibles. Sélectionnez le mode que vous voulez configurer : **Background** (Arrière-plan), **Best Effort** (Meilleur effort), **Video** (Vidéo) ou **Voice** (Voix). Suivez les instructions pour le mode que vous avez sélectionné.

Background (Arrière-plan)

Use Aggregation (Utiliser l'agrégation) Cette option détermine si la couche Media Access Control (MAC) configurera ou non une session Add Block Acknowledgement (ADDBA). La valeur par défaut est **No** (Non). Sélectionnez **Yes** (Oui) pour activer cette option.

Accept Aggregation (Accepter l'agrégation) Cette option détermine si la couche MAC acceptera ou non une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre max. de paquets de l'agrégation) Cette option détermine le nombre maximum de paquets (sous-trames) dans le regroupement. La plage varie de **0** à **7**. La valeur par défaut est **7**.

Max. Aggregation Size (Taille max. d'agrégation) Cette option détermine la taille maximum du regroupement (en octets). La plage varie de **0** à **16 000**. La valeur par défaut est **12 000**.

Timeout Internal (Période d'inactivité) Cette option définit la période d'inactivité durant laquelle le regroupement devrait être fermé avec une « condition de fermeture » avant qu'il soit fermé par le temporisateur. La plage varie de **0** à **100** ms. La valeur par défaut est **3**.

Min. Size of Packet in Aggregation (Taille min. des paquets de l'agrégation) Cette option détermine la taille minimum (en octets) des paquets pouvant être accumulés dans le regroupement. La plage varie de **0** à **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai ADDBA) Cette option détermine la durée après laquelle la requête ADDBA se termine, s'il n'y a aucun échange de trames à l'intérieur du délai selon l'accord Block Acknowledgement (ACK). La plage varie de **0** à **65 535** ms. La valeur par défaut est **0**, qui désactive le délai.

Aggregation Window Size (Taille de la fenêtre d'agrégation) Cette option détermine le nombre maximum de paquets transmis sans obtenir d'accusé de réception. La plage varie de **0** à **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Best Effort (Meilleur effort)

Use Aggregation (Utiliser l'agrégation) Cette option détermine si la couche Media Access Control (MAC) configurera ou non une session Add Block Acknowledgement (ADDBA). La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Accept Aggregation (Accepter l'agrégation) Cette option détermine si la couche MAC acceptera ou non une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre max. de paquets de l'agrégation) Cette option détermine le nombre maximum de paquets (sous-trames) dans le regroupement. La plage varie de **0** à **10**. La valeur par défaut est **10**.

Max. Aggregation Size (Taille max. d'agrégation) Cette option détermine la taille maximum du regroupement (en octets). La plage varie de **0** à **20 000**. La valeur par défaut est **16 000**.

Timeout Internal (Période d'inactivité) Cette option définit la période d'inactivité durant laquelle le regroupement devrait être fermé avec une « condition de fermeture » avant qu'il soit fermé par le temporisateur. La plage varie de **0** à **100** ms. La valeur par défaut est **3**.

Min. Size of Packet in Aggregation (Taille min. des paquets de l'agrégation) Cette option détermine la taille minimum (en octets) des paquets pouvant être accumulés dans le regroupement. La plage varie de **0** à **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai ADDBA) Cette option détermine la durée après laquelle la requête ADDBA se termine, s'il n'y a aucun échange de trames à l'intérieur du délai selon l'accord Block Acknowledgement (ACK). La plage varie de **0** à **65 535** ms. La valeur par défaut est **0**, qui désactive le délai.

Aggregation Window Size (Taille de la fenêtre d'agrégation) Cette option détermine le nombre maximum de paquets transmis sans obtenir d'accusé de réception. La plage varie de **0** à **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Video (Vidéo)

Use Aggregation (Utiliser l'agrégation) Cette option détermine si la couche Media Access Control (MAC) configurera ou non une session Add Block Acknowledgement (ADDBA). La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Accept Aggregation (Accepter l'agrégation) Cette option détermine si la couche MAC acceptera ou non une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre max. de paquets de l'agrégation) Cette option détermine le nombre maximum de paquets (sous-trames) dans le regroupement. La plage varie de **0** à **7**. La valeur par défaut est **7**.

Max. Aggregation Size (Taille max. d'agrégation) Cette option détermine la taille maximum du regroupement (en octets). La plage varie de **0** à **16 000**. La valeur par défaut est **12 000**.

Timeout Internal (Période d'inactivité) Cette option définit la période d'inactivité durant laquelle le regroupement devrait être fermé avec une « condition de fermeture » avant qu'il soit fermé par le temporisateur. La plage varie de **0** à **100** ms. La valeur par défaut est **3**.

Min. Size of Packet in Aggregation (Taille min. des paquets de l'agrégation) Cette option détermine la taille minimum (en octets) des paquets pouvant être accumulés dans le regroupement. La plage varie de **0** à **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai ADDBA) Cette option détermine la durée après laquelle la requête ADDBA se termine, s'il n'y a aucun échange de trames à l'intérieur du délai selon l'accord Block Acknowledgement (ACK). La plage varie de **0** à **65 535** ms. La valeur par défaut est **0**, qui désactive le délai.

Aggregation Window Size (Taille de la fenêtre d'agrégation) Cette option détermine le nombre maximum de paquets transmis sans obtenir d'accusé de réception. La plage varie de **0** à **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Voice (Voix)

Use Aggregation (Utiliser l'agrégation) Cette option détermine si la couche Media Access Control (MAC) configurera ou non une session Add Block Acknowledgement (ADDBA). La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Accept Aggregation (Accepter l'agrégation) Cette option détermine si la couche MAC acceptera ou non une requête ADDBA. La valeur par défaut est **Yes** (Oui). Sélectionnez **No** (Non) pour désactiver cette option.

Max. Number of Packets in Aggregation (Nombre max. de paquets de l'agrégation) Cette option détermine le nombre maximum de paquets (sous-trames) dans le regroupement. La plage varie de **0** à **2**. La valeur par défaut est **2**.

Max. Aggregation Size (Taille max. d'agrégation) Cette option détermine la taille maximum du regroupement (en octets). La plage varie de **0** à **16 000**. La valeur par défaut est **10 000**.

Timeout Internal (Période d'inactivité) Cette option définit la période d'inactivité durant laquelle le regroupement devrait être fermé avec une « condition de fermeture » avant qu'il soit fermé par le temporisateur. La plage varie de **0** à **100** ms. La valeur par défaut est **10**.

Min. Size of Packet in Aggregation (Taille min. des paquets de l'agrégation) Cette option détermine la taille minimum (en octets) des paquets pouvant être accumulés dans le regroupement. La plage varie de **0** à **1 500**. La valeur par défaut est **10**.

ADDBA Timeout (Délai ADDBA) Cette option détermine la durée après laquelle la requête ADDBA se termine, s'il n'y a aucun échange de trames à l'intérieur du délai selon l'accord Block Acknowledgement (ACK). La plage varie de **0** à **65 535** ms. La valeur par défaut est **0**, qui désactive le délai.

Aggregation Window Size (Taille de la fenêtre d'agrégation) Cette option détermine le nombre maximum de paquets transmis sans obtenir d'accusé de réception. La plage varie de **0** à **64**. La valeur par défaut est **64**.

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Wireless (Sans fil) > Advanced Wireless Settings (Paramètres sans fil avancés)

Configurez les fonctions sans fil avancées du pont. La configuration devrait être confiée à un administrateur réseau car des paramètres incorrects peuvent réduire les performances des transmissions sans fil.



REMARQUE
Les paramètres de l'écran *Advanced Wireless Settings* (Paramètres sans fil avancés) sont conçus pour les utilisateurs avancés seulement.

Advanced Wireless (Paramètres sans fil avancés)

Use LDPC (Utiliser LDPC) Active ou désactive la correction des erreurs par codes de contrôle de parité à basse densité (Low-Density Parity-Check Code, LDPC), qui permet de réduire la probabilité de perte de données dans des canaux de transmission avec bruit. L'algorithme d'adaptation du taux de transmission désactive le codage LDPC lorsque le taux de transmission PHY est élevé (au-dessus de 162). Pour utiliser le schéma avancé de correction des erreurs LDCP, conservez la valeur par défaut **Yes** (Oui). Sinon, sélectionnez **No** (Non).

ERP Protection Type (Type de protection ERP) Cette option configure la protection des paquets OFDM, malgré la présence des stations 802.11b dans le réseau sans fil. En envoyant des paquets RTS/CTS ou CTS2Self dans les débits 802.11b, le pont informe le réseau sans fil que des paquets OFDM seront transférés et protège les paquets dans le réseau sans fil. Les paquets RTS/CTS et CTS2Self créent du trafic, qui peut entraîner des débits moins élevés.

L'option RTS/CTS offre une meilleure protection mais un débit plus lent lorsque comparé à CTS2Self, parce que l'option RTS/CTS exige une réponse provenant de l'appareil recevant les données. Pour utiliser l'option RTS/CTS, conservez la valeur par défaut, **RTS/CTS**. L'option None (Aucune) peut causer des collisions entre paquets OFDM et CCK. Pour utiliser l'option None (Aucune), sélectionnez **None** (Aucune). Pour utiliser l'option CTS2Self, sélectionnez **CTS2Self**.

11n Protection Type (Protection de type 11n) Cette option configure la protection contre les périphériques ne prenant pas en charge le haut débit (non-High Throughput, HT) du réseau sans fil. Dans le cas d'un routeur sans fil (ou d'un point d'accès), cette option permet de détecter l'association avec un périphérique moins récent ne prenant pas en charge le haut débit (HT) et informe le périphérique d'utiliser les mécanismes RTS/CTS ou CTS2Self avant chaque transmission de données. Cette fonction prend aussi en charge toutes les protections incluses dans la norme 802.11n, y compris MIMO.

L'option RTS/CTS offre une meilleure protection mais un débit plus lent lorsque comparé à CTS2Self, parce que l'option RTS/CTS exige une réponse provenant de l'appareil recevant les données. Pour utiliser l'option RTS/CTS, conservez la valeur par défaut, **RTS/CTS**. L'option None (Aucune) peut causer des collisions entre les paquets HT et les paquets échangés avec des appareils plus anciens. Pour utiliser l'option None (Aucune), sélectionnez **None** (Aucune). Pour utiliser l'option CTS2Self, sélectionnez **CTS2Self**.

Percentage of maximal transmit power (Pourcentage de la puissance de transmission maximale) Cette option configure le pourcentage de puissance maximale de transmission relativement aux restrictions du domaine de réglementation. Par exemple, si les restrictions du domaine de réglementation autorisent des transmissions pouvant atteindre 20 dB, alors un pourcentage de 50 % permettrait une transmission maximale de 10 dB. Sélectionnez le pourcentage que vous voulez utiliser : **12 %**, **25 %**, **50 %** ou **100 %**. La valeur par défaut est **100 %**.

QoS Classification Type (Type de classification de la qualité de service) Cette option configure le mappage 802.1D ou 802.1Q, des champs IP DSCP/TOS aux priorités WMM (Background (Arrière-plan), Best Effort (Meilleur effort), Video (Vidéo) ou Voice (Voix)). Conservez la valeur par défaut **802.1D** ou sélectionnez **802.1Q**, qui est utilisée par certains flux IPTV.

Re-establish Ethernet connection when initiating wireless connection (Établir de nouveau la connexion Ethernet lors de l'initiation de la connexion sans fil) Pour déclencher la détection DHCP à partir de l'appareil situé derrière le pont, le pont réinitialisera le lien Ethernet entre lui-même et l'appareil chaque fois qu'une connexion sans fil est établie. Pour désactiver cette fonction, sélectionnez **No** (Non). Sinon, conservez la sélection par défaut, soit **Yes** (Oui).

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Administration > Management (Gestion)

Utilisez cet écran pour gérer les fonctions du pont : accès à l'utilitaire Web-, sauvegarde du fichier de configuration du routeur et redémarrage.



Management (Gestion)

Bridge Access (Accès au pont)

Utilisez un mot de passe pour protéger l'accès à l'utilitaire Web.

Bridge Password (Mot de passe du routeur) Entrez un nouveau mot de passe pour le pont.

Re-enter to confirm (Confirmation du mot de passe) Entrez de nouveau le mot de passe pour le confirmer.

Idle Timeout (Période d'inactivité) La session de configuration est fermée automatiquement après la période d'inactivité spécifiée ici. La plage varie de **60** à **3 600** secondes. La valeur par défaut est **600**.

Web Access (Accès Web)

Access via Wireless (Accès sans fil) Si vous utilisez le pont dans un domaine public pour permettre l'accès sans fil à vos invités, vous pouvez désactiver l'accès sans fil à l'utilitaire Web du pont. Dans ce cas, l'accès à l'utilitaire ne sera possible que par une connexion câblée. Conservez la sélection par défaut, soit **Enabled** (Activé), pour permettre l'accès sans fil à l'utilitaire; sinon, sélectionnez **Disabled** (Désactivé).

Backup (Sauvegarder) et Restore (Rétablir)

Backup (Sauvegarder) Cliquez sur **Backup Configurations** (Sauvegarder les configurations) pour sauvegarder la configuration du pont dans un fichier. Suivez ensuite les instructions affichées à l'écran.

Restore (Rétablir) Cliquez sur **Browse** (Parcourir), puis sélectionnez le fichier de configuration. Cliquez ensuite sur **Restore Configurations** (Rétablir les configurations).

System Reboot (Redémarrage du système)

Reboot (Redémarrer) Pour redémarrer le pont, cliquez sur **Start to Reboot** (Lancer le redémarrage).

Cliquez sur **Save Settings** (Enregistrer les paramètres) pour appliquer les changements ou sur **Cancel Changes** (Annuler les modifications) pour les annuler.

Administration > Factory Defaults (Paramètres par défaut d'usine)

Cet écran permet de restaurer la configuration du pont à ses paramètres par défaut d'usine.

Factory Defaults (Paramètres par défaut d'usine)

Restore All Settings (Restaurer tous les paramètres) Pour réinitialiser les paramètres du pont aux valeurs par défaut, cliquez sur **Restore All Settings**. Le rétablissement des paramètres par défaut supprime tous les paramètres personnalisés.



Administration > Upgrade Firmware (Mise à niveau du microcode)

Utilisez cet écran pour mettre à niveau le microcode du pont. Il est recommandé d'éviter de mettre à niveau le microcode, sauf si vous ne parvenez pas à faire fonctionner le pont ou si le nouveau microcode offre des fonctions que vous voulez utiliser.



Pour mettre à niveau le microcode, téléchargez le fichier du microcode sur le site de Linksys, à l'adresse **www.linksys.com/support**.

Upgrade Firmware (Mise à niveau du microcode)

Please select a file to upgrade the firmware (Sélectionner un fichier pour la mise à niveau du microcode) Cliquez sur **Browse** (Parcourir) et sélectionnez le fichier de mise à niveau du microcode. Ensuite, cliquez sur **Start to Upgrade** (Mettre à niveau) et suivez les instructions affichées à l'écran.

Status (État) > Bridge (Pont)

L'état actuel du pont est affiché.



Bridge Information (Informations sur le pont)

Firmware Version (Version du microcode) La version actuelle du microcode du pont est affichée.

Local Network (Réseau local)

Local MAC Address (Adresse MAC locale) L'adresse MAC du pont, telle que vue par votre réseau Ethernet local, est affichée.

IP Address (Adresse IP) L'adresse IP du pont, telle que vue par votre réseau Ethernet local, est affichée.

Subnet Mask (Masque de sous-réseau) Indique l'adresse du masque de sous-réseau de votre réseau local.

Status (État) > Wireless (Sans fil)

Des renseignements sur votre réseau sans fil sont affichés.



Wireless (Sans fil)

Link Status (État du lien) L'état de la connexion à votre réseau sans fil est affiché.

MAC Address (Adresse MAC) L'adresse MAC du pont, telle que vue par votre réseau sans fil local, est affichée.

Network Name (SSID) (Nom du réseau - SSID) Indique le nom du réseau sans fil, ou SSID.

BSSID L'adresse MAC sans fil du routeur sans fil connecté (ou du point d'accès) est affichée.

Radio Band (Bande radio) La bande radio de votre réseau sans fil est affichée.

Channel Width (Largeur de canal) La largeur de canal utilisée par votre réseau sans fil est affichée en MHz.

Wide Channel (Canal large) Selon les réglages de canal de votre routeur, le canal large est affiché. Si vous sélectionnez le paramètre de bande radio ou de largeur de canal Wide - 40MHz Channel (Canal large de 40 MHz), ce paramètre est alors disponible pour le canal principal sans fil N.

Standard Channel (Canal standard) Indique le canal standard. Si vous sélectionnez le paramètre de bande radio ou de largeur de canal Wide - 40MHz Channel (Canal large de 40 MHz), le canal standard devient un canal secondaire du réseau sans fil N.

Bit Rate (Débit binaire) Le taux de transmission des données est affiché.

Signal Le pourcentage de la puissance du signal est affiché. 100 % est la puissance de signal la plus forte et 0 % est la plus faible possible.

Security (Sécurité) La méthode de sécurité utilisée par votre réseau sans fil est affichée.

Dépannage

WES610N/WET610N

Votre ordinateur ou un autre périphérique Ethernet câblé ne communique pas avec le routeur sans fil.

1. Accédez à l'utilitaire Web du pont.
2. Assurez-vous que le nom du réseau (SSID) correspond au nom de votre réseau sans fil dans l'écran *Basic Wireless Settings* (Paramètres sans fil de base).
3. Assurez-vous que les paramètres de sécurité (WPA, WPA2 ou WEP) correspondent aux paramètres de sécurité de votre réseau sans fil.

L'adresse IP du pont doit être changée.

Si le pont est connecté à un réseau doté d'un serveur DHCP (il s'agit généralement d'un routeur), alors le serveur DHCP fournira une adresse IP au pont. Si aucun serveur DHCP n'est disponible, alors le pont utilisera son adresse IP statique par défaut, soit **169.254.1.250**.

Si vous désirez que le pont utilise une adresse IP statique en tout temps, alors suivez ces instructions :

1. Accédez à l'utilitaire Web du pont.
2. Cliquez sur l'onglet **Network Setup** (Configuration réseau).
3. Dans le menu déroulant *Network Connection Type* (Type de connexion réseau), sélectionnez **Static IP** (Adresse IP statique).
4. Remplissez les champs *Static IP Address* (Adresse IP statique), *Subnet Mask* (Masque de sous-réseau) et *Default Gateway* (Passerelle par défaut).
5. Cliquez sur **Save Settings** (Enregistrer les paramètres).

L'ordinateur branché au pont ou un à autre périphérique Ethernet câblé n'arrive pas à entrer en communication avec des périphériques sans fil (comme un ordinateur ou une imprimante).

Vérifiez les points suivants :

- Assurez-vous que le périphérique sans fil se trouve sur le même réseau sans fil que l'ordinateur ou l'autre périphérique Ethernet câblé qui est branché au pont.
- Assurez-vous que le même nom de réseau (SSID) est utilisé par tous les périphériques utilisant le réseau sans fil.
- Assurez-vous que tous les périphériques sont configurés avec le même réseau IP et utilisent des adresses IP compatibles.

L'utilitaire Web n'accepte pas votre mot de passe.

Vérifiez les points suivants :

- Le système distingue les minuscules et les majuscules dans les mots de passe. Assurez-vous de respecter les caractères majuscules et minuscules lorsque vous entrez le mot de passe.
- Si vous avez oublié votre mot de passe, vous pouvez réinitialiser le pont à ses paramètres par défaut.

 Appuyez sur le bouton **Reset** (Réinitialiser) du pont pendant approximativement cinq secondes. Le mot de passe par défaut, **admin**, sera rétabli. Tous les autres réglages du pont seront aussi réinitialisés à leurs valeurs par défaut. (Pour accéder à l'utilitaire Web, entrez **admin** dans le champ *Password* (Mot de passe).)

Après avoir apporté des modifications avec l'utilitaire Web, les nouveaux paramètres ne sont pas affichés.

Cliquez sur **Actualiser** dans le navigateur Web. Si les nouveaux paramètres ne sont pas affichés, procédez comme suit :

1. Déconnectez l'adaptateur d'alimentation du pont.
2. Attendez cinq secondes, puis branchez l'adaptateur d'alimentation de nouveau dans le pont.
3. Cliquez sur **Actualiser** dans le navigateur Web.

RESSOURCES WEB
Si vous n'avez pas trouvé de réponse à vos questions, consultez la section d'assistance de notre site Web, à l'adresse **Linksys.com/support**

Spécifications

WES610N

Modèle	WES610N
Normes	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Voyants	Alimentation, Ethernet, Wi-Fi Protected Setup™ (configuration d'accès Wi-Fi protégé), liaison sans fil, activités et liaisons Ethernet individuelles
Ports	Ethernet (4), alimentation
Touches	Reset (Réinitialiser), Wi-Fi Protected Setup (Configuration de l'accès Wi-Fi protégé)
Câblage	CAT5e
Nombre d'antennes	3 (internes)
Type de connecteur d'antenne	s. o.
Amovible (Oui/Non)	Non
Modulations	802.11a : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b : CCK/QPSK, BPSK 802.11g : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n : OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Puiss. RF (EIRP) en dBm	802.11a : 15 dBm (type) @ 54 Mbit/s 802.11b : 19 dBm (type) @ 11 Mbit/s 802.11g : 16 dBm (type) @ 54 Mbit/s 802.11n (2,4 GHz): 18 dBm (type) @ MCS15 802.11n (5 GHz) : 16 dBm (type) @ MCS15
Sensibilité de réception	802.11a : -72 dBm (type) @ 54 Mbit/s 802.11b : -85 dBm (type) @ 11 Mbit/s 802.11g : -73 dBm (type) @ 54 Mbit/s 802.11n (20 MHz) : -75 dBm (type) @ MCS15 802.11n (40 MHz) : -69 dBm (type) @ MCS15
Gain d'antenne en dBi	1
Sécurité sans fil	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bits de clé de sécurité	Cryptage de données jusqu'à 128 bits

Environnement d'exploitation

Dimensions	177 mm x 128 mm x 68 mm (6,97 po x 5,04 po x 2,68 po)
Poids	295 g (0,65 lb)
Certification	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/préliminaire n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentation	12 V, 1 A
Températures de fonctionnement	0 à 40 °C (32 à 104 °F)
Températures de stockage	-20 à 60 °C (-4 à 140 °F)
Humidité (fonctionnement)	10 à 85 %, sans condensation
Humidité (entreposage)	5 à 90 %, sans condensation

Les spécifications peuvent changer sans préavis.

WET610N

Modèle	WET610N
Normes	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Voyants	Alimentation, Ethernet, Wi-Fi Protected Setup™, sans fil
Ports	Ethernet, alimentation
Touches	Reset (Réinitialiser), Wi-Fi Protected Setup (Configuration de l'accès Wi-Fi protégé)
Câblage	CAT5e
Nombre d'antennes	3 (internes)
Type de connecteur d'antenne	s. o.
Amovible (Oui/Non)	Non
Modulations	802.11a : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b : CCK/QPSK, BPSK 802.11g : OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n : OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Puiss. RF (EIRP) en dBm	802.11a : 15 dBm (type) @ 54 Mbit/s 802.11b : 18 dBm (type) @ 11 Mbit/s 802.11g : 16 dBm (type) @ 54 Mbit/s 802.11n : 12 dBm (typical) @ 130 Mbit/s (HT20), 270 Mbit/s (HT40)
Sensibilité de réception	802.11a : -72 dBm (type) @ 54 Mbit/s 802.11b : -85 dBm (type) @ 11 Mbit/s 802.11g : -73 dBm (type) @ 54 Mbit/s 802.11n : -70 dBm (type) @ MCS15/2,4 GHz, -69 dBm (type) @ MCS15/5,0 GHz
Gain d'antenne en dBi	1
Sécurité sans fil	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bits de clé de sécurité	Cryptage de données jusqu'à 128 bits

Environnement d'exploitation

Dimensions	145 mm x 106 mm x 52 mm (5,71 po x 4,17 po x 2,05 po)
Poids	159 g (5,61 oz)
Certification	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/préliminaire n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentation	12 V, 1 A
Températures de fonctionnement	0 à 40 °C (32 à 104 °F)
Températures de stockage	-20 à 60 °C (-4 à 140 °F)
Humidité (fonctionnement)	10 à 85 %, sans condensation
Humidité (entreposage)	5 à 90 %, sans condensation

Les spécifications peuvent changer sans préavis.

Linksys.com/support

Cisco, le logo Cisco et Linksys sont des marques de commerce ou des marques déposées de Cisco ou de ses sociétés affiliées aux États-Unis et dans d'autres pays.
Vous trouverez une liste des marques de commerce de Cisco à l'adresse www.cisco.com/go/trademarks. Les autres marques mentionnées dans ce document sont la propriété de leur détenteur respectif.

© Cisco et ses sociétés affiliées, 2011. Tous droits réservés.

3425-01249



Οδηγός χρήσης

Linksys WET610N/WES610N | Γέφυρα Dual-Band N Entertainment

Περιεχόμενα

Επισκόπηση προϊόντος

Ταμπλό λυχνιών LED 2
Ταμπλό θυρών 3

Λίστα ελέγχου ασύρματης ασφάλειας

Αλλαγή του προεπιλεγμένου ονόματος ασύρματου δικτύου ή SSID 4
Αλλαγή του προεπιλεγμένου κωδικού πρόσβασης 4
Ενεργοποίηση του φιλτραρίσματος διευθύνσεων MAC 4
Ενεργοποίηση κρυπτογράφησης 4
Γενικές οδηγίες ασφάλειας δικτύου 4
Επιπλέον συμβουλές ασφάλειας 5

Σύνθετη διαμόρφωση

Πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα 6
Setup (Ρύθμιση) > Basic Setup (Βασική ρύθμιση) 7
Language (Γλώσσα) 7
Network Setup (Ρύθμιση δικτύου) 7
Wireless (Ασύρματη σύνδεση) > Basic Wireless Settings (Βασικές ρυθμίσεις ασύρματης σύνδεσης). 7
Basic Wireless Settings (Βασικές ρυθμίσεις ασύρματης σύνδεσης) 8
Wireless Security (Ασύρματη ασφάλεια) 8
Wi-Fi Protected Setup 9
Wireless (Ασύρματη σύνδεση) > Wireless Network Site Survey (Έρευνα τοποθεσιών ασύρματου δικτύου) 10
Wireless Network Site Survey (Έρευνα τοποθεσιών ασύρματου δικτύου) 10
Wireless (Ασύρματη σύνδεση) > WMM® 11
WMM 12
Wireless (Ασύρματη σύνδεση) > Advanced Wireless Settings (Σύνθετες ρυθμίσεις ασύρματης σύνδεσης). 13
Advanced Wireless (Σύνθετες ασύρματες ρυθμίσεις) 14
Administration (Διαχείριση) > Management (Διαχείριση λειτουργιών). 14
Management (Διαχείριση λειτουργιών) 14
Administration (Διαχείριση) > Factory Defaults (Εργοστασιακές ρυθμίσεις) 15
Factory Defaults (Εργοστασιακές ρυθμίσεις) 15
Administration (Διαχείριση) > Upgrade Firmware (Αναβάθμιση υλικολογισμικού). 15
Upgrade Firmware (Αναβάθμιση υλικολογισμικού) 15
Status (Κατάσταση) > Bridge (Γέφυρα) 16
Bridge Information (Πληροφορίες γέφυρας) 16
Local Network (Τοπικό δίκτυο) 16
Status (Κατάσταση) > Wireless (Ασύρματη σύνδεση) 16
Wireless (Ασύρματη σύνδεση) 16

Αντιμετώπιση προβλημάτων

WES610N/WET610N 17

Προδιαγραφές

WES610N 18
WET610N 19

Επισκόπηση προϊόντος

Σας ευχαριστούμε που επιλέξατε τη γέφυρα Dual-Band N Entertainment της Linksys. Η γέφυρα προσφέρει τη δυνατότητα σύνδεσης οποιασδήποτε συσκευής ενσύρματης σύνδεσης Ethernet στο ασύρματο δίκτυό σας. Η γέφυρα βασίζεται σε Wireless-N διπλής ζώνης, οπότε είναι συμβατή με οποιονδήποτε δρομολογητή ή σημείο πρόσβασης Wireless-N, -G, -A ή -B. Για την πρώτη εγκατάσταση, ακολουθήστε τα βήματα που περιγράφονται στο φάκελο του CD. Για τη διαμόρφωση των σύνθετων ρυθμίσεων, χρησιμοποιήστε το πρακτικό διαδικτυακό βοηθητικό πρόγραμμα.

Ταμπλό λυχνιών LED



WES610N

WET610N

Ασύρματη σύνδεση (μπλε) Η λυχνία αυτή ανάβει όταν υπάρχει ασύρματη σύνδεση. Αναβοσβήνει όταν η γέφυρα πραγματοποιεί αποστολή ή λήψη δεδομένων μέσω του ασύρματου δικτύου.

Κουμπί Wi-Fi Protected Setup Εάν ο δρομολογητής του δικτύου σας υποστηρίζει Wi-Fi Protected Setup και χρησιμοποιεί ασφάλεια WPA ή WPA2, μπορείτε να χρησιμοποιήσετε το Wi-Fi Protected Setup για αυτόματη σύνδεση της γέφυρας. Για να χρησιμοποιήσετε το Wi-Fi Protected Setup, ανατρέξτε στην ενότητα "Wireless (Ασύρματη σύνδεση) > Basic Wireless Settings (Βασικές ρυθμίσεις ασύρματης σύνδεσης)" στη σελίδα 7.

Wi-Fi Protected Setup (μπλε/πορτοκαλί) Η λυχνία αυτή αναβοσβήνει με μπλε χρώμα για δύο λεπτά κατά τη διάρκεια του Wi-Fi Protected Setup. Ανάβει σταθερά με μπλε χρώμα, όταν είναι ενεργοποιημένη η ασφάλεια ασύρματης σύνδεσης. Εάν προκύψει σφάλμα κατά τη διαδικασία του Wi-Fi Protected Setup, η λυχνία LED ανάβει με πορτοκαλί χρώμα. Βεβαιωθείτε ότι ο δρομολογητής του δικτύου υποστηρίζει Wi-Fi Protected Setup. Περιμένετε μέχρι να απενεργοποιηθεί η λυχνία LED και στη συνέχεια προσπαθήστε ξανά.

Ethernet (μπλε) Η λυχνία αυτή ανάβει όταν υπάρχει ενσύρματη σύνδεση. Αναβοσβήνει όταν η γέφυρα πραγματοποιεί αποστολή ή λήψη δεδομένων μέσω των θυρών Ethernet.

Λειτουργία (μπλε) Η λυχνία αυτή αναβοσβήνει κατά την ενεργοποίηση της γέφυρας.

Ταμπλό θυρών



WES610N WET610N

Ethernet Οι θύρες Ethernet συνδέουν τη γέφυρα με έναν υπολογιστή ή άλλη συσκευή του δικτύου Ethernet. Το μοντέλο WES610N έχει τέσσερις θύρες και το μοντέλο WET610N μία θύρα.

Επαναφορά Υπάρχουν δύο τρόποι για να πραγματοποιήσετε επαναφορά της γέφυρας στις εργοστασιακές ρυθμίσεις. Πατήστε παρατεταμένα το κουμπί επαναφοράς για περίπου πέντε δευτερόλεπτα ή πραγματοποιήστε επαναφορά των προεπιλογών από την οθόνη Administration (Διαχείριση) > Factory Defaults (Εργοστασιακές ρυθμίσεις) του διαδικτυακού βοηθητικού προγράμματος της γέφυρας. Το μοντέλο WES610N έχει ένα κουμπί επαναφοράς στην κάτω πλευρά, ενώ το μοντέλο WET610N ένα κουμπί επαναφοράς στο πίσω ταμπλό θυρών.

Τροφοδοσία Η θύρα τροφοδοσίας συνδέει τη γέφυρα με το συνοδευτικό καλώδιο τροφοδοσίας.

Λίστα ελέγχου ασύρματης ασφάλειας

Τα ασύρματα δίκτυα είναι πρακτικά και εύκολα στην εγκατάσταση και τα σπίτια που διαθέτουν πρόσβαση υψηλής ταχύτητας στο Internet τα υιοθετούν με γρήγορους ρυθμούς. Επειδή η λειτουργία των ασύρματων δικτύων γίνεται με την αποστολή πληροφοριών μέσω ραδιοκυμάτων, ενδέχεται να είναι πιο ευάλωτα σε εισβολείς σε σχέση με το παραδοσιακό ενσύρματο δίκτυο. Μπορεί να γίνει υποκλοπή των σημάτων του ασύρματου δικτύου σας, όπως μπορεί να γίνει και με τα σήματα του κινητού ή ασύρματου τηλεφώνου σας. Επειδή δεν μπορείτε να εμποδίσετε με φυσικό τρόπο τη σύνδεση κάποιου στο ασύρματο δίκτυό σας, πρέπει να λάβετε μερικά επιπλέον μέτρα για να διατηρήσετε ασφαλές το δίκτυό σας.

Αλλαγή του προεπιλεγμένου ονόματος ασύρματου δικτύου ή SSID

Οι ασύρματες συσκευές διαθέτουν ένα προεπιλεγμένο όνομα ασύρματου δικτύου ή SSID, το οποίο ορίζεται από το εργοστάσιο. Αυτό είναι το όνομα του ασύρματου δικτύου σας και μπορεί να έχει μήκος έως και 32 χαρακτήρες. Τα ασύρματα προϊόντα της Linksys χρησιμοποιούν το όνομα **linksys** ως το προεπιλεγμένο όνομα ασύρματου δικτύου. Θα πρέπει να αλλάξετε το όνομα ασύρματου δικτύου σε κάποια μοναδική λέξη, προκειμένου να μπορείτε να ξεχωρίσετε το ασύρματο δίκτυό σας από τα υπόλοιπα ασύρματα δίκτυα που ενδέχεται να βρίσκονται γύρω σας, αλλά δεν πρέπει να χρησιμοποιήσετε προσωπικές πληροφορίες για το σκοπό αυτό (όπως τον αριθμό κοινωνικής ασφάλισης) επειδή αυτές οι πληροφορίες ενδέχεται να είναι διαθέσιμες σε οποιονδήποτε πραγματοποιεί αναζήτηση για ασύρματα δίκτυα.

Αλλαγή του προεπιλεγμένου κωδικού πρόσβασης

Για τα ασύρματα προϊόντα, όπως σημεία πρόσβασης και δρομολογητές, θα σας ζητηθεί να εισαγάγετε έναν κωδικό πρόσβασης εάν προσπαθήσετε να αλλάξετε τις ρυθμίσεις τους. Οι συσκευές αυτές διαθέτουν έναν προεπιλεγμένο κωδικό πρόσβασης, ο οποίος έχει οριστεί από το εργοστάσιο. Ο προεπιλεγμένος κωδικός πρόσβασης Linksys είναι **admin**. Οι χάκερς γνωρίζουν αυτές τις προεπιλεγμένες ρυθμίσεις και ενδέχεται να προσπαθήσουν να τις χρησιμοποιήσουν για να αποκτήσουν πρόσβαση στο ασύρματο δίκτυό σας και να αλλάξουν τις ρυθμίσεις του δικτύου σας. Για να αποτρέψετε τυχόν μη εξουσιοδοτημένες αλλαγές, προσαρμόστε τον κωδικό πρόσβασης της συσκευής ώστε να μην είναι εύκολο για κάποιον να τον μαντέψει.

Ενεργοποίηση του φιλτραρίσματος διευθύνσεων MAC

Οι δρομολογητές της Linksys σάς δίνουν τη δυνατότητα να ενεργοποιήσετε το φιλτράρισμα διευθύνσεων MAC. Η διεύθυνση MAC αποτελείται από μια μοναδική ακολουθία αριθμών και γραμμάτων που εκχωρείται σε κάθε συσκευή δικτύου. Εάν είναι ενεργοποιημένο το φιλτράρισμα διευθύνσεων MAC, η πρόσβαση στο ασύρματο δίκτυο επιτρέπεται μόνο σε ασύρματες συσκευές που διαθέτουν συγκεκριμένες διευθύνσεις MAC. Μπορείτε, για παράδειγμα, να καθορίσετε τη διεύθυνση MAC όλων των υπολογιστών του σπιτιού σας, ώστε μόνο οι συγκεκριμένοι υπολογιστές να έχουν δυνατότητα πρόσβασης στο ασύρματο δίκτυό σας.

Ενεργοποίηση κρυπτογράφησης

Η κρυπτογράφηση προστατεύει τα δεδομένα που μεταδίδονται μέσω ασύρματου δικτύου. Τα πρότυπα Wi-Fi Protected Access (WPA/WPA2) και Wired Equivalent Privacy (WEP) προσφέρουν διαφορετικά επίπεδα ασφάλειας για ασύρματες επικοινωνίες.

Ένα δίκτυο που διαθέτει κρυπτογράφηση WPA/WPA2 είναι ασφαλέστερο από ένα δίκτυο με κρυπτογράφηση WEP, επειδή η κρυπτογράφηση WPA/WPA2 χρησιμοποιεί δυναμικό κλειδί κρυπτογράφησης. Για να προστατεύσετε τις πληροφορίες καθώς μεταφέρονται μέσω ραδιοκυμάτων, θα πρέπει να έχετε ενεργοποιήσει το υψηλότερο επίπεδο κρυπτογράφησης που υποστηρίζεται από τον εξοπλισμό του δικτύου σας.

Το WEP είναι παλιότερο πρότυπο κρυπτογράφησης και ενδέχεται να είναι η μόνη διαθέσιμη επιλογή σε κάποιες παλαιότερες συσκευές που δεν υποστηρίζουν το πρότυπο WPA.

Γενικές οδηγίες ασφάλειας δικτύου

Η ασφάλεια ασύρματου δικτύου είναι άχρηστη εάν το ίδιο το δίκτυο δεν είναι ασφαλές.

- Προστατεύστε με κωδικό πρόσβασης όλους τους υπολογιστές του δικτύου σας και χρησιμοποιήστε επιπλέον κωδικούς πρόσβασης για να προστατεύσετε όλα τα σημαντικά αρχεία.
- Αλλάζετε τακτικά κωδικούς πρόσβασης.
- Εγκαταστήστε λογισμικό προστασίας από ιούς και προσωπικό τείχος προστασίας.
- Απενεργοποιήστε τη λειτουργία διαμοιρασμού αρχείων (ομότιμη λειτουργία). Ορισμένες εφαρμογές ενδέχεται να ενεργοποιούν το διαμοιρασμό αρχείων χωρίς τη συγκατάθεση ή/και τη γνώση σας.

Επιπλέον συμβουλές ασφάλειας

- Κρατήστε τους ασύρματους δρομολογητές, τα σημεία πρόσβασης ή τις πύλες μακριά από εξωτερικούς τοίχους και παράθυρα.
- Απενεργοποιείτε τους ασύρματους δρομολογητές, τα σημεία πρόσβασης ή τις πύλες όταν δεν τα χρησιμοποιείτε (τη νύχτα ή όταν λείπετε για διακοπές).
- Χρησιμοποιείτε ισχυρές φράσεις πρόσβασης με μήκος τουλάχιστον οχτώ χαρακτήρων. Να συνδυάζετε γράμματα και αριθμούς ώστε να αποφύγετε τη χρήση συνηθισμένων λέξεων που μπορεί κάποιος να βρει στο λεξικό.

Σύνθετη διαμόρφωση

Αφού ολοκληρώσετε την εγκατάσταση της γέφυρας ακολουθώντας τα βήματα που περιγράφονται στο φάκελο του CD, η γέφυρα θα είναι έτοιμη προς χρήση. Ωστόσο, εάν θελήσετε να αλλάξετε τις σύνθετες ρυθμίσεις, χρησιμοποιήστε το διαδικτυακό βοηθητικό πρόγραμμα της γέφυρας. Το κεφάλαιο αυτό περιγράφει όλες τις ιστοσελίδες του βοηθητικού προγράμματος, καθώς και τις βασικές λειτουργίες κάθε σελίδας. Μπορείτε να αποκτήσετε πρόσβαση στο βοηθητικό πρόγραμμα μέσω ενός προγράμματος περιήγησης στον ιστό από έναν υπολογιστή που είναι συνδεδεμένος με τη γέφυρα.

Το διαδικτυακό βοηθητικό πρόγραμμα έχει τις ακόλουθες βασικές καρτέλες: Setup (Ρύθμιση), Wireless (Ασύρματη σύνδεση), Administration (Διαχείριση) και Status (Κατάσταση). Μπορείτε να έχετε πρόσβαση σε επιπλέον καρτέλες αφού κάνετε κλικ σε κάποια από τις κύριες καρτέλες.

Πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα

Χρησιμοποιήστε ένα πρόγραμμα περιήγησης στον ιστό για να προσπελάσετε το διαδικτυακό βοηθητικό πρόγραμμα.

Εάν η γέφυρα είναι συνδεδεμένη σε ένα δίκτυο με ένα διακομιστή DHCP (συνήθως το δρομολογητή του δικτύου), θα λάβει τη διεύθυνση IP της από το διακομιστή DHCP. Εάν δεν υπάρχει διακομιστής DHCP, η γέφυρα θα χρησιμοποιήσει την προεπιλεγμένη στατική διεύθυνση IP της, **169.254.1.250**. (Εάν ορίσετε μια μόνιμη στατική διεύθυνση IP στη γέφυρα μέσω του διαδικτυακού βοηθητικού προγράμματος, εισαγάγετε αντ' αυτής τη στατική διεύθυνση IP.)

ΣΗΜΕΙΩΣΗ
Εάν δεν γνωρίζετε τη διεύθυνση IP της γέφυρας, μπορείτε να τη βρείτε στον πίνακα πελατών DHCP του δρομολογητή σας. (Ανατρέξτε στην τεκμηρίωση του δρομολογητή σας.)

Εάν δεν μπορείτε να εντοπίσετε τη διεύθυνση IP της γέφυρας, μπορείτε να πραγματοποιήσετε επαναφορά της γέφυρας. Πατήστε το κουμπί **Reset** (Επαναφορά) στη γέφυρα για περίπου πέντε δευτερόλεπτα, χρησιμοποιώντας το άκρο ενός ανοιγμένου συνδετήρα. Με τη διαδικασία αυτή, η γέφυρα επαναφέρεται στις εργοστασιακά προεπιλεγμένες ρυθμίσεις. Η γέφυρα θα ζητήσει μια διεύθυνση IP από το διακομιστή DHCP (συνήθως το δρομολογητή του δικτύου). Εάν δεν εντοπιστεί διακομιστής DHCP, η γέφυρα θα χρησιμοποιήσει την προεπιλεγμένη στατική διεύθυνση IP της, **169.254.1.250**, μέχρι να εντοπίσει ένα διακομιστή DHCP και να λάβει από αυτόν μια δυναμική διεύθυνση IP.

Εάν η γέφυρα δεν είναι συσχετισμένη με ένα δρομολογητή και χρησιμοποιεί τις εργοστασιακά προεπιλεγμένες ρυθμίσεις, συνδέστε έναν υπολογιστή στη γέφυρα, χρησιμοποιώντας σύνδεση Ethernet για να προσπελάσετε το διαδικτυακό βοηθητικό πρόγραμμα. Θα πρέπει να διαμορφώσετε τη σύνδεση Ethernet στον υπολογιστή με μια στατική διεύθυνση IP και μια μάσκα υποδικτύου.

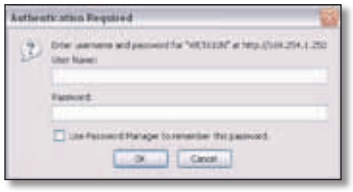
Η διεύθυνση IP του προσαρμογέα Ethernet θα πρέπει να ρυθμιστεί σε συγκεκριμένη διεύθυνση IP.

1. Στο πεδίο *IP address* (Διεύθυνση IP), πληκτρολογήστε **169.254.x.y** (το x θα πρέπει να αντικατασταθεί από έναν αριθμό μεταξύ 1 και 254, και το y από έναν αριθμό μεταξύ 0 και 255).
2. Στο πεδίο *Subnet mask* (Μάσκα υποδικτύου), πληκτρολογήστε **255.255.0.0**.

ΣΗΜΕΙΩΣΗ
Τα βήματα για την εκχώρηση στατικής διεύθυνσης IP στον προσαρμογέα Ethernet στον υπολογιστή σας ποικίλλουν ανάλογα με το λειτουργικό σύστημα. Για οδηγίες, ανατρέξτε στην τεκμηρίωση βοήθειας του δικού σας λειτουργικού συστήματος.

Αφού εκχωρήσετε μια στατική διεύθυνση IP στον προσαρμογέα Ethernet, εκκινήστε το πρόγραμμα περιήγησης στον ιστό του υπολογιστή σας και εισαγάγετε τη διεύθυνση IP του προσαρμογέα (η προεπιλεγμένη ρύθμιση είναι **169.254.1.250**) στο πεδίο *Address* (Διεύθυνση). Πατήστε **Enter**.

Εμφανίζεται μια οθόνη αιτήματος κωδικού πρόσβασης. (Αν το λειτουργικό σας σύστημα δεν είναι Windows XP, θα δείτε μια παρόμοια οθόνη.) Αφήστε το πεδίο *User name* (Όνομα χρήστη) κενό. Εισαγάγετε τον κωδικό πρόσβασης που δημιουργήσατε κατά τα βήματα του Οδηγού εγκατάστασης. Εάν δεν δημιουργήσατε νέο κωδικό πρόσβασης, χρησιμοποιήστε τον προεπιλεγμένο κωδικό πρόσβασης **admin**. (Μπορείτε να ορίσετε νέο κωδικό πρόσβασης στην καρτέλα *Administration* (Διαχείριση) > οθόνη *Management* (Διαχείριση λειτουργιών).) Πατήστε **OK** για να συνεχίσετε.



ΣΗΜΕΙΩΣΗ
Εάν δεν εμφανιστεί η οθόνη αιτήματος κωδικού πρόσβασης, περιμένετε δύο λεπτά και προσπαθήστε ξανά.

Setup (Ρύθμιση) > Basic Setup (Βασική ρύθμιση)

Πρώτα εμφανίζεται η οθόνη *Basic Setup* (Βασική ρύθμιση). Χρησιμοποιήστε αυτήν την οθόνη για να αλλάξετε τη γλώσσα του διαδικτυακού βοηθητικού προγράμματος ή να αλλάξετε τις ρυθμίσεις ενσύρματου δικτύου Ethernet της γέφυρας.





Language (Γλώσσα)

Language (Γλώσσα) Χρησιμοποιήστε αυτήν την επιλογή για να ρυθμίσετε τη γλώσσα του διαδικτυακού βοηθητικού προγράμματος. Επιλέξτε την επιθυμητή γλώσσα από το αναπτυσσόμενο μενού.

Network Setup (Ρύθμιση δικτύου)

Στην ενότητα αυτή καθορίζεται εάν η διεύθυνση IP της γέφυρας λαμβάνεται αυτόματα από ένα διακομιστή DHCP, για παράδειγμα, το δρομολογητή του δικτύου σας (Automatic Configuration - DHCP (Αυτόματη διαμόρφωση - DHCP) ή ρυθμίζεται με μη αυτόματο τρόπο (Static IP (Στατική διεύθυνση IP)).

Bridge IP (IP γέφυρας) Εάν το δίκτυό σας διαθέτει διακομιστή DHCP, για παράδειγμα, το δρομολογητή του δικτύου σας, ο οποίος εκχωρεί διευθύνσεις IP στις συσκευές δικτύου σας, διατηρήστε την προεπιλογή **Automatic Configuration - DHCP** (Αυτόματη διαμόρφωση - DHCP). Η γέφυρα θα ζητήσει μια διεύθυνση IP από το διακομιστή DHCP (συνήθως το δρομολογητή του δικτύου). Εάν δεν εντοπιστεί διακομιστής DHCP, η γέφυρα θα χρησιμοποιήσει την προεπιλεγμένη στατική διεύθυνση IP της, **169.254.1.250**, μέχρι να εντοπίσει ένα διακομιστή DHCP και να λάβει από αυτόν μια δυναμική διεύθυνση IP.

Εάν θέλετε να ορίσετε μια μόνιμη στατική διεύθυνση IP για τη γέφυρα, επιλέξτε **Static IP** (Στατική διεύθυνση IP).

Εάν επιλέξετε τη ρύθμιση Static IP (Στατική διεύθυνση IP), συμπληρώστε τα ακόλουθα πεδία:

- **Static IP Address** (Στατική διεύθυνση IP) Εισαγάγετε μια μοναδική διεύθυνση IP, η οποία θα χρησιμοποιείται για την πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα.
- **Subnet Mask** (Μάσκα υποδικτύου) Εισαγάγετε τη μάσκα υποδικτύου του ενσύρματου δικτύου σας.
- **Default Gateway** (Προεπιλεγμένη πύλη) Εισαγάγετε τη διεύθυνση IP της προεπιλεγμένης πύλης για το δίκτυό σας (στις περισσότερες περιπτώσεις, η πύλη αυτή είναι ο δρομολογητής σας).

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να εφαρμόσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Wireless (Ασύρματη σύνδεση) > Basic Wireless Settings (Βασικές ρυθμίσεις ασύρματης σύνδεσης)

Χρησιμοποιήστε την οθόνη *Basic Wireless Settings* (Βασικές ρυθμίσεις ασύρματης σύνδεσης) για να διαμορφώσετε τις βασικές ρυθμίσεις ασύρματης σύνδεσης και ασφαλείας της γέφυρας.

Υπάρχουν δύο τρόποι διαμόρφωσης των ρυθμίσεων της γέφυρας: Manual (Μη αυτόματα) και Wi-Fi Protected Setup. Η λειτουργία Wi-Fi Protected Setup διευκολύνει τη ρύθμιση του ασύρματου δικτύου σας. Εάν ο δρομολογητής του δικτύου σας υποστηρίζει Wi-Fi Protected Setup και χρησιμοποιεί ασφάλεια WPA ή WPA2, μπορείτε να χρησιμοποιήσετε το Wi-Fi Protected Setup για αυτόματη σύνδεση της γέφυρας.

Configuration View (Προβολή διαμόρφωσης) Για να διαμορφώσετε με μη αυτόματο τρόπο το ασύρματο δίκτυό σας, επιλέξτε **Manual** (Μη αυτόματα). Ανατρέξτε στην ενότητα **Basic Wireless Settings** (Βασικές ρυθμίσεις ασύρματης σύνδεσης), **σελίδα 8**. Για να χρησιμοποιήσετε το Wi-Fi Protected Setup, επιλέξτε **Wi-Fi Protected Setup**. Ανατρέξτε στην ενότητα **Wi-Fi Protected Setup**, **σελίδα 9**.

Basic Wireless Settings (Βασικές ρυθμίσεις ασύρματης σύνδεσης)



Network Name (SSID) (Όνομα δικτύου (SSID)) Το SSID είναι το κοινό όνομα δικτύου που χρησιμοποιούν όλα τα σημεία ενός ασύρματου δικτύου. Το SSID πρέπει να είναι το ίδιο σε όλες τις συσκευές του ασύρματου δικτύου. Κάνει διάκριση πεζών-κεφαλαίων και δεν πρέπει να υπερβαίνει τους 32 χαρακτήρες πληκτρολογίου (μπορείτε να χρησιμοποιήσετε οποιονδήποτε από τους χαρακτήρες του πληκτρολογίου). Βεβαιωθείτε ότι η ρύθμιση αυτή αντιστοιχεί στη ρύθμιση του ασύρματου δρομολογητή/σημείου πρόσβασης. Για πρόσθετη ασφάλεια, θα πρέπει να αλλάξετε το προεπιλεγμένο SSID (**linksys**) σε ένα μοναδικό όνομα.

Wireless Security (Ασύρματη ασφάλεια)

Η γέφυρα υποστηρίζει τις ακόλουθες επιλογές ασύρματης ασφάλειας: WPA Personal (Προσωπικό WPA), WPA2 Personal (Προσωπικό WPA2) και WEP. Τα WPA (Wi-Fi Protected Access) και WPA2 αποτελούν ισχυρότερες μεθόδους ασφάλειας σε σύγκριση με το WEP (Wired Equivalent Privacy). Για περισσότερες πληροφορίες σχετικά με την ασύρματη ασφάλεια, ανατρέξτε στην ενότητα "Λίστα ελέγχου ασύρματης ασφάλειας", σελίδα 4.

Security Mode (Λειτουργία ασφάλειας)

Επιλέξτε τη μέθοδο ασφάλειας που είναι η κατάλληλη για το ασύρματο δίκτυό σας. Εάν δεν θέλετε να χρησιμοποιήσετε την ασύρματη ασφάλεια, διατηρήστε την προεπιλεγμένη τιμή **Disabled** (Απενεργοποιημένη).

ΣΗΜΕΙΩΣΗ
Να θυμάστε πως κάθε συσκευή του ασύρματου δικτύου σας ΠΡΕΠΕΙ να χρησιμοποιεί την ίδια μέθοδο και την ίδια φράση πρόσβασης/κλειδί ασφάλειας. Σε αντίθετη περίπτωση δεν θα είναι δυνατή η επικοινωνία μεταξύ των ασύρματων συσκευών.

WPA Personal (Προσωπικό WPA)

Το WPA είναι ένα πρότυπο ασφαλείας ισχυρότερο από την κρυπτογράφηση WEP.



Encryption (Κρυπτογράφηση) Το WPA υποστηρίζει τη μέθοδο κρυπτογράφησης TKIP, με δυναμικά κλειδιά κρυπτογράφησης.

Passphrase (Φράση πρόσβασης) Εισαγάγετε το κλειδί που μοιράζεται η γέφυρα με τον ασύρματο δρομολογητή/το σημείο πρόσβασης. Θα πρέπει να έχει 8-63 χαρακτήρες.

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

WPA2 Personal (Προσωπικό WPA2)

Η λειτουργία WPA2 είναι μια πιο σύνθετη και πιο ασφαλής μορφή της λειτουργίας WPA.



Encryption (Κρυπτογράφηση) Το WPA2 υποστηρίζει δύο μεθόδους κρυπτογράφησης, τις TKIP και AES, με δυναμικά κλειδιά κρυπτογράφησης. Επιλέξτε τη μέθοδο κρυπτογράφησης, **AES** ή **TKIP ή AES**. Η προεπιλεγμένη ρύθμιση είναι **AES**.

Passphrase (Φράση πρόσβασης) Εισαγάγετε το κλειδί που μοιράζεται η γέφυρα με τον ασύρματο δρομολογητή/το σημείο πρόσβασης. Θα πρέπει να έχει 8-63 χαρακτήρες.

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

WEP

Το WEP είναι μια βασική μέθοδος κρυπτογράφησης, η οποία δεν είναι τόσο ασφαλής όσο το WPA ή το WPA2.



Encryption (Κρυπτογράφηση) Ορίστε ένα επίπεδο κρυπτογράφησης WEP, **40/64 bits (10 hex digits)** (40/64-bit (10 δεκαεξαδικά ψηφία)) ή **104/128 bits (26 hex digits)** (104/128-bit (26 δεκαεξαδικά ψηφία)). Το προεπιλεγμένο επίπεδο είναι **40/64 bits (10 hex digits)** (40/64-bit (10 δεκαεξαδικά ψηφία)).

Key 1 (Κλειδί 1) Εισαγάγετε το κλειδί WEP του δικτύου σας.

Tx Key (Κλειδί Tx) Το **Key 1** (Κλειδί 1) είναι το κλειδί μετάδοσης που χρησιμοποιείται από τη γέφυρα.

Authentication (Έλεγχος ταυτότητας) Η προεπιλεγμένη ρύθμιση είναι **Auto** (Αυτόματα), η οποία επιτρέπει να χρησιμοποιηθεί έλεγχος ταυτότητας σε μορφή Ανοικτού συστήματος ή Κοινόχρηστου κλειδιού. Επιλέξτε **Open** (Ανοικτό) για χρήση του ελέγχου ταυτότητας ανοικτού συστήματος. Ο αποστολέας και ο παραλήπτης δεν χρησιμοποιούν κλειδί WEP για τον έλεγχο ταυτότητας. Επιλέξτε **Shared** (Κοινόχρηστο) για χρήση του ελέγχου ταυτότητας κοινόχρηστου κλειδιού. Ο αποστολέας και ο παραλήπτης χρησιμοποιούν κλειδί WEP για τον έλεγχο ταυτότητας.

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Wi-Fi Protected Setup

Υπάρχουν δύο διαθέσιμες μέθοδοι. Χρησιμοποιήστε τη μέθοδο που αντιστοιχεί στο δρομολογητή που χρησιμοποιείτε.





Μέθοδος 1

Χρησιμοποιήστε αυτή τη μέθοδο εάν ο δρομολογητής σας διαθέτει κουμπί Wi-Fi Protected Setup.

1. Πατήστε το κουμπί **Wi-Fi Protected Setup** στο δρομολογητή.
2. Εντός δύο λεπτών, πατήστε το κουμπί **Wi-Fi Protected Setup** στην οθόνη *Wi-Fi Protected Setup* της γέφυρας.
3. Μετά τη διαμόρφωση της γέφυρας, πατήστε **Close** (Κλείσιμο).

Η οθόνη *Wi-Fi Protected Setup* εμφανίζει τα εξής στοιχεία: Link Status (Κατάσταση σύνδεσης), Network Name (SSID) (Όνομα δικτύου (SSID)) και Security method (Μέθοδος ασφάλειας).

Μέθοδος 2

Χρησιμοποιήστε αυτή τη μέθοδο αν ο δρομολογητής σας ζητά τον αριθμό PIN της γέφυρας.

1. Στην οθόνη *Wi-Fi Protected Setup* του **δρομολογητή**, εισαγάγετε τον αριθμό PIN στην οθόνη *Wi-Fi Protected Setup* της **γέφυρας**. Έπειτα, επιλέξτε **Register** (Εγγραφή) ή πατήστε το αντίστοιχο κουμπί. (Αναγράφεται επίσης στην κάτω πλευρά της γέφυρας.)
2. Στην οθόνη *Wi-Fi Protected Setup* της **γέφυρας**, πατήστε **OK**.
3. Μετά τη διαμόρφωση της γέφυρας, πατήστε **Close** (Κλείσιμο).

Η οθόνη *Wi-Fi Protected Setup* εμφανίζει τα εξής στοιχεία: Link Status (Κατάσταση σύνδεσης), Network Name (SSID) (Όνομα δικτύου (SSID)) και Security method (Μέθοδος ασφαλείας).

Wireless (Ασύρματη σύνδεση) > Wireless Network Site Survey (Έρευνα τοποθεσιών ασύρματου δικτύου)

Κάντε κλικ στην καρτέλα **Wireless Network Site Survey** (Έρευνα τοποθεσιών ασύρματου δικτύου) για να ξεκινήσετε μια έρευνα τοποθεσιών. Η οθόνη *Wireless Network Site Survey* (Έρευνα τοποθεσιών ασύρματου δικτύου) εμφανίζει τα ασύρματα δίκτυα που ανιχνεύτηκαν από τη γέφυρα.



Wireless Network Site Survey (Έρευνα τοποθεσιών ασύρματου δικτύου)

Number of Wireless Networks (Αριθμός ασύρματων δικτύων) Εμφανίζεται ο αριθμός των ασύρματων δικτύων που ανιχνεύτηκαν από τη γέφυρα.

Select (Επιλογή) Για να συνδεθείτε σε ένα ασύρματο δίκτυο, πατήστε **Select** (Επιλογή). Στη συνέχεια, πατήστε **Connect** (Σύνδεση).

Wireless Network Name (Όνομα ασύρματου δικτύου) Εμφανίζεται το όνομα δικτύου ή SSID του ασύρματου δικτύου.

GHz Εμφανίζεται η ζώνη συχνοτήτων του ασύρματου δικτύου.

Signal (Σήμα) Εμφανίζεται το ποσοστό ισχύος του σήματος. Η ένδειξη 100% αντιστοιχεί στο ισχυρότερο δυνατό σήμα, ενώ η ένδειξη 0% στο πιο αδύναμο σήμα.

Security (Ασφάλεια) Εάν το δίκτυο υποστηρίζει Wi-Fi Protected Setup, εμφανίζεται το εικονίδιο του Wi-Fi Protected Setup . Εμφανίζεται η μέθοδος ασφάλειας που χρησιμοποιείται από το ασύρματο δίκτυο.

Κάντε κλικ στο **Refresh** (Ανανέωση) για να ενημερώσετε τις πληροφορίες που εμφανίζονται στην οθόνη.

Αφού επιλέξετε ένα δίκτυο, επιλέξτε **Connect** (Σύνδεση). Θα εμφανιστεί μια νέα οθόνη. Ακολουθήστε τις οδηγίες για τη μέθοδο ασφάλειας του δικτύου σας.

WPA



Network Name (SSID) (Όνομα δικτύου (SSID)) Εμφανίζεται αυτόματα το όνομα του δικτύου που επιλέξατε.

Security Mode (Λειτουργία ασφάλειας) Εμφανίζεται αυτόματα η ρύθμιση WPA Personal (Προσωπικό WPA).

Encryption (Κρυπτογράφηση) Το WPA υποστηρίζει τη μέθοδο κρυπτογράφησης TKIP, με δυναμικά κλειδιά κρυπτογράφησης.

Passphrase (Φράση πρόσβασης) Εισαγάγετε το κλειδί που μοιράζεται η γέφυρα με τον ασύρματο δρομολογητή/το σημείο πρόσβασης. Θα πρέπει να έχει 8-63 χαρακτήρες.

Κάντε κλικ στο **Refresh** (Ανανέωση) για να ενημερώσετε τις πληροφορίες που εμφανίζονται στην οθόνη.

Αφού εισαγάγετε τις ρυθμίσεις ασφάλειας, επιλέξτε **Connect** (Σύνδεση).

WPA2



Network Name (SSID) (Όνομα δικτύου (SSID)) Εμφανίζεται αυτόματα το όνομα του δικτύου που επιλέξατε.

Security Mode (Λειτουργία ασφάλειας) Εμφανίζεται αυτόματα η ρύθμιση WPA2 Personal (Προσωπικό WPA2).

Encryption (Κρυπτογράφηση) Το WPA2 υποστηρίζει δύο μεθόδους κρυπτογράφησης, τις TKIP και AES, με δυναμικά κλειδιά κρυπτογράφησης. Επιλέξτε τη μέθοδο κρυπτογράφησης, **AES** ή **TKIP ή AES**.

Passphrase (Φράση πρόσβασης) Εισαγάγετε το κλειδί που μοιράζεται η γέφυρα με τον ασύρματο δρομολογητή/το σημείο πρόσβασης. Θα πρέπει να έχει 8-63 χαρακτήρες.

Κάντε κλικ στο **Refresh** (Ανανέωση) για να ενημερώσετε τις πληροφορίες που εμφανίζονται στην οθόνη.

Αφού εισαγάγετε τις ρυθμίσεις ασφάλειας, επιλέξτε **Connect** (Σύνδεση).

WEP



Network Name (SSID) (Όνομα δικτύου (SSID)) Εμφανίζεται αυτόματα το όνομα του δικτύου που επιλέξατε.

Security Mode (Λειτουργία ασφάλειας) Εμφανίζεται αυτόματα η ρύθμιση WEP.

Encryption (Κρυπτογράφηση) Ορίστε ένα επίπεδο κρυπτογράφησης WEP, **40/64 bits (10 hex digits)** (40/64-bit (10 δεκαεξαδικά ψηφία)) ή **104/128 bits (26 hex digits)** (104/128-bit (26 δεκαεξαδικά ψηφία)).

Key 1 (Κλειδί 1) Εισαγάγετε το κλειδί WEP του δικτύου σας.

Tx Key (Κλειδί Tx) Το **Key 1** (Κλειδί 1) είναι το κλειδί μετάδοσης που χρησιμοποιείται από τη γέφυρα.

Authentication (Έλεγχος ταυτότητας) Η προεπιλεγμένη ρύθμιση είναι **Auto** (Αυτόματα), η οποία επιτρέπει να χρησιμοποιηθεί έλεγχος ταυτότητας σε μορφή Ανοικτού συστήματος ή Κοινόχρηστου κλειδιού. Επιλέξτε **Open** (Ανοικτό) για χρήση του ελέγχου ταυτότητας ανοικτού συστήματος. Ο αποστολέας και ο παραλήπτης δεν χρησιμοποιούν κλειδί WEP για τον έλεγχο ταυτότητας. Επιλέξτε **Shared** (Κοινόχρηστο) για χρήση του ελέγχου ταυτότητας κοινόχρηστου κλειδιού. Ο αποστολέας και ο παραλήπτης χρησιμοποιούν κλειδί WEP για τον έλεγχο ταυτότητας.

Κάντε κλικ στο **Refresh** (Ανανέωση) για να ενημερώσετε τις πληροφορίες που εμφανίζονται στην οθόνη.

Αφού εισαγάγετε τις ρυθμίσεις ασφάλειας, επιλέξτε **Connect** (Σύνδεση).

Wireless (Ασύρματη σύνδεση) > WMM®

Διαμορφώστε τις ρυθμίσεις Wireless MultiMedia (WMM). Το WMM θέτει προτεραιότητες στα πακέτα, ανάλογα με την αντίστοιχη λειτουργία πρόσβασης καθενός (τύπος κίνησης): Background (Φόντο), Best Effort (Καλύτερη προσπάθεια), Video (Βίντεο) ή Voice (Φωνή). Η προσαρμογή αυτών των ρυθμίσεων θα πρέπει να γίνεται μόνο από ειδικευμένο διαχειριστή, καθώς οι εσφαλμένες ρυθμίσεις μπορεί να μειώσουν την απόδοση του ασύρματου δικτύου.



ΣΗΜΕΙΩΣΗ
Οι ρυθμίσεις στην οθόνη *WMM* προορίζονται μόνο για προχωρημένους χρήστες.

WMM

Λειτουργία πρόσβασης

Μπορείτε να ορίσετε διαφορετικές ρυθμίσεις για τις τέσσερις διαθέσιμες λειτουργίες πρόσβασης. Επιλέξτε τη λειτουργία που θέλετε να διαμορφώσετε: **Background** (Φόντο), **Best Effort** (Καλύτερη προσπάθεια), **Video** (Βίντεο) ή **Voice** (Φωνή). Ακολουθήστε τις οδηγίες για τη λειτουργία που θα επιλέξετε.

Background (Φόντο)

Use Aggregation (Χρήση συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο Media Access Control (MAC) θα ρυθμίσει ή όχι μια περίοδο λειτουργίας Add Block Acknowledgement (ADDBA). Η προεπιλογή είναι **No** (Όχι). Επιλέξτε **Yes** (Ναι) για να ενεργοποιήσετε αυτήν την επιλογή.

Accept Aggregation (Αποδοχή συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο MAC θα αποδεχθεί ή όχι ένα αίτημα ADDBA. Η προεπιλογή είναι **Yes** (Ναι). Επιλέξτε **No** (Όχι) για να απενεργοποιήσετε αυτήν την επιλογή.

Max. Number of Packets in Aggregation (Μέγιστος αριθμός πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων (επιμέρους πλαισίων) στο σύνολο. Το εύρος είναι **0** έως **7**. Η προεπιλεγμένη τιμή είναι **7**.

Max. Aggregation Size (Μέγιστο μέγεθος συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο μέγεθος του συνόλου (σε bytes). Το εύρος είναι **0** έως **16000**. Η προεπιλεγμένη τιμή είναι **12000**.

Timeout Internal (Εσωτερικό χρονικό όριο) Η επιλογή αυτή καθορίζει το χρονικό όριο μετά το οποίο θα πρέπει να κλείσει το σύνολο με μια "συνθήκη κλεισίματος", πριν το κλείσει ο χρονοδιακόπτης. Το εύρος είναι **0** έως **100** ms. Η προεπιλεγμένη τιμή είναι **3**.

Min. Size of Packet in Aggregation (Ελάχιστο μέγεθος πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το ελάχιστο μέγεθος (σε bytes) των πακέτων που θα συναθροιστούν στο σύνολο. Το εύρος είναι **0** έως **1500**. Η προεπιλεγμένη τιμή είναι **10**.

ADDBA Timeout (Χρονικό όριο ADDBA) Η επιλογή αυτή καθορίζει τη χρονική περίοδο μετά την οποία τερματίζεται η ρύθμιση ADDBA, εάν δεν υπάρχουν ανταλλαγές πλαισίου εντός της διάρκειας αυτής από τη συμφωνία Block Acknowledgement (ACK). Το εύρος είναι **0** έως **65535** ms. Η προεπιλεγμένη τιμή είναι **0**, τιμή που απενεργοποιεί το χρονικό όριο.

Aggregation Window Size (Μέγεθος παραθύρου συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων που μεταδίδονται χωρίς λήψη ACK. Το εύρος είναι **0** έως **64**. Η προεπιλεγμένη τιμή είναι **64**.

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Best Effort (Καλύτερη προσπάθεια)

Use Aggregation (Χρήση συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο Media Access Control (MAC) θα ρυθμίσει ή όχι μια περίοδο λειτουργίας Add Block Acknowledgement (ADDBA). Η προεπιλογή είναι **Yes** (Ναι). Επιλέξτε **No** (Όχι) για να απενεργοποιήσετε αυτήν την επιλογή.

Accept Aggregation (Αποδοχή συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο MAC θα αποδεχθεί ή όχι ένα αίτημα ADDBA. Η προεπιλογή είναι **Yes** (Ναι). Επιλέξτε **No** (Όχι) για να απενεργοποιήσετε αυτήν την επιλογή.

Max. Number of Packets in Aggregation (Μέγιστος αριθμός πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων (επιμέρους πλαισίων) στο σύνολο. Το εύρος είναι **0** έως **10**. Η προεπιλεγμένη τιμή είναι **10**.

Max. Aggregation Size (Μέγιστο μέγεθος συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο μέγεθος του συνόλου (σε bytes). Το εύρος είναι **0** έως **20000**. Η προεπιλεγμένη τιμή είναι **16000**.

Timeout Internal (Εσωτερικό χρονικό όριο) Η επιλογή αυτή καθορίζει το χρονικό όριο μετά το οποίο θα πρέπει να κλείσει το σύνολο με μια "συνθήκη κλεισίματος", πριν το κλείσει ο χρονοδιακόπτης. Το εύρος είναι **0** έως **100** ms. Η προεπιλεγμένη τιμή είναι **3**.

Min. Size of Packet in Aggregation (Ελάχιστο μέγεθος πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το ελάχιστο μέγεθος (σε bytes) των πακέτων που θα συναθροιστούν στο σύνολο. Το εύρος είναι **0** έως **1500**. Η προεπιλεγμένη τιμή είναι **10**.

ADDBA Timeout (Χρονικό όριο ADDBA) Η επιλογή αυτή καθορίζει τη χρονική περίοδο μετά την οποία τερματίζεται η ρύθμιση ADDBA, εάν δεν υπάρχουν ανταλλαγές πλαισίου εντός της διάρκειας αυτής από τη συμφωνία Block Acknowledgement (ACK). Το εύρος είναι **0** έως **65535** ms. Η προεπιλεγμένη τιμή είναι **0**, τιμή που απενεργοποιεί το χρονικό όριο.

Aggregation Window Size (Μέγεθος παραθύρου συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων που μεταδίδονται χωρίς λήψη ACK. Το εύρος είναι **0** έως **64**. Η προεπιλεγμένη τιμή είναι **64**.

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Video (Βίντεο)

Use Aggregation (Χρήση συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο Media Access Control (MAC) θα ρυθμίσει ή όχι μια περίοδο λειτουργίας Add Block Acknowledgement (ADDBA). Η προεπιλογή είναι **Yes** (Ναι). Επιλέξτε **No** (Όχι) για να απενεργοποιήσετε αυτήν την επιλογή.

Accept Aggregation (Αποδοχή συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο MAC θα αποδεχθεί ή όχι ένα αίτημα ADDBA. Η προεπιλογή είναι **Yes** (Ναι). Επιλέξτε **No** (Όχι) για να απενεργοποιήσετε αυτήν την επιλογή.

Max. Number of Packets in Aggregation (Μέγιστος αριθμός πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων (επιμέρους πλαισίων) στο σύνολο. Το εύρος είναι **0** έως **7**. Η προεπιλεγμένη τιμή είναι **7**.

Max. Aggregation Size (Μέγιστο μέγεθος συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο μέγεθος του συνόλου (σε bytes). Το εύρος είναι **0** έως **16000**. Η προεπιλεγμένη τιμή είναι **12000**.

Timeout Internal (Εσωτερικό χρονικό όριο) Η επιλογή αυτή καθορίζει το χρονικό όριο μετά το οποίο θα πρέπει να κλείσει το σύνολο με μια "συνθήκη κλεισίματος", πριν το κλείσει ο χρονοδιακόπτης. Το εύρος είναι **0** έως **100** ms. Η προεπιλεγμένη τιμή είναι **3**.

Min. Size of Packet in Aggregation (Ελάχιστο μέγεθος πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το ελάχιστο μέγεθος (σε bytes) των πακέτων που θα συναθροιστούν στο σύνολο. Το εύρος είναι **0** έως **1500**. Η προεπιλεγμένη τιμή είναι **10**.

ADDBA Timeout (Χρονικό όριο ADDBA) Η επιλογή αυτή καθορίζει τη χρονική περίοδο μετά την οποία τερματίζεται η ρύθμιση ADDBA, εάν δεν υπάρχουν ανταλλαγές πλαισίου εντός της διάρκειας αυτής από τη συμφωνία Block Acknowledgement (ACK). Το εύρος είναι **0** έως **65535** ms. Η προεπιλεγμένη τιμή είναι **0**, τιμή που απενεργοποιεί το χρονικό όριο.

Aggregation Window Size (Μέγεθος παραθύρου συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων που μεταδίδονται χωρίς λήψη ACK. Το εύρος είναι **0** έως **64**. Η προεπιλεγμένη τιμή είναι **64**.

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Voice (Φωνή)

Use Aggregation (Χρήση συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο Media Access Control (MAC) θα ρυθμίσει ή όχι μια περίοδο λειτουργίας Add Block Acknowledgement (ADDBA). Η προεπιλογή είναι **Yes** (Ναι). Επιλέξτε **No** (Όχι) για να απενεργοποιήσετε αυτήν την επιλογή.

Accept Aggregation (Αποδοχή συνάθροισης) Η επιλογή αυτή καθορίζει εάν το επίπεδο MAC θα αποδεχθεί ή όχι ένα αίτημα ADDBA. Η προεπιλογή είναι **Yes** (Ναι). Επιλέξτε **No** (Όχι) για να απενεργοποιήσετε αυτήν την επιλογή.

Max. Number of Packets in Aggregation (Μέγιστος αριθμός πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων (επιμέρους πλαισίων) στο σύνολο. Το εύρος είναι **0** έως **2**. Η προεπιλεγμένη τιμή είναι **2**.

Max. Aggregation Size (Μέγιστο μέγεθος συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο μέγεθος του συνόλου (σε bytes). Το εύρος είναι **0** έως **16000**. Η προεπιλεγμένη τιμή είναι **10000**.

Timeout Internal (Εσωτερικό χρονικό όριο) Η επιλογή αυτή καθορίζει το χρονικό όριο μετά το οποίο θα πρέπει να κλείσει το σύνολο με μια "συνθήκη κλεισίματος", πριν το κλείσει ο χρονοδιακόπτης. Το εύρος είναι **0** έως **100** ms. Η προεπιλεγμένη τιμή είναι **10**.

Min. Size of Packet in Aggregation (Ελάχιστο μέγεθος πακέτων σε συνάθροιση) Η επιλογή αυτή καθορίζει το ελάχιστο μέγεθος (σε bytes) των πακέτων που θα συναθροιστούν στο σύνολο. Το εύρος είναι **0** έως **1500**. Η προεπιλεγμένη τιμή είναι **10**.

ADDBA Timeout (Χρονικό όριο ADDBA) Η επιλογή αυτή καθορίζει τη χρονική περίοδο μετά την οποία τερματίζεται η ρύθμιση ADDBA, εάν δεν υπάρχουν ανταλλαγές πλαισίου εντός της διάρκειας αυτής από τη συμφωνία Block Acknowledgement (ACK). Το εύρος είναι **0** έως **65535** ms. Η προεπιλεγμένη τιμή είναι **0**, τιμή που απενεργοποιεί το χρονικό όριο.

Aggregation Window Size (Μέγεθος παραθύρου συνάθροισης) Η επιλογή αυτή καθορίζει το μέγιστο αριθμό πακέτων που μεταδίδονται χωρίς λήψη ACK. Το εύρος είναι **0** έως **64**. Η προεπιλεγμένη τιμή είναι **64**.

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Wireless (Ασύρματη σύνδεση) > Advanced Wireless Settings (Σύνθετες ρυθμίσεις ασύρματης σύνδεσης)

Διαμορφώστε τις σύνθετες ασύρματες λειτουργίες της γέφυρας. Η προσαρμογή αυτών των ρυθμίσεων θα πρέπει να γίνεται μόνο από ειδικευμένο διαχειριστή, καθώς οι εσφαλμένες ρυθμίσεις μπορεί να μειώσουν την απόδοση του ασύρματου δικτύου.



ΣΗΜΕΙΩΣΗ
Οι ρυθμίσεις στην οθόνη *Advanced Wireless Settings* (Σύνθετες ρυθμίσεις ασύρματης σύνδεσης) προορίζονται μόνο για προχωρημένους χρήστες.

Advanced Wireless (Σύνθετες ασύρματες ρυθμίσεις)

Use LDPC (Χρήση LDPC) Ο κώδικας Low-Density Parity-Check Code (LDPC) ενεργοποιεί ή απενεργοποιεί τη διόρθωση σφαλμάτων με στόχο τη μείωση της πιθανότητας απώλειας δεδομένων σε θορυβώδη κανάλια. Ο αλγόριθμος προσαρμογής ρυθμού (Rate Adaptation) απενεργοποιεί αυτόματα την κωδικοποίηση LDPC κατά την εργασία σε υψηλούς ρυθμούς PHY (πάνω από 162). Για να χρησιμοποιήσετε το προηγμένο σχέδιο διόρθωσης σφάλματος LDCP, διατηρήστε την προεπιλεγμένη ρύθμιση **Yes** (Ναι). Διαφορετικά, επιλέξτε **No** (Όχι).

ERP Protection Type (Τύπος προστασίας ERP) Η επιλογή αυτή διαμορφώνει την προστασία των πακέτων OFDM παρά την παρουσία σταθμών 802.11b εντός του ασύρματου δικτύου. Με την αποστολή πακέτων RTS/CTS ή CTS2Self σε ρυθμούς 802.11b, η γέφυρα ενημερώνει το ασύρματο δίκτυο ότι τα πακέτα OFDM πρόκειται να μεταφερθούν και προστατεύει τα πακέτα στο ασύρματο δίκτυο. Τα πακέτα RTS/CTS και CTS2Self δημιουργούν επιβάρυνση, η οποία ενδέχεται να καταλήξει σε χαμηλότερες ταχύτητες μεταγωγής.

Η επιλογή RTS/CTS παρέχει καλύτερη κάλυψη αλλά χαμηλότερες ταχύτητες μεταγωγής σε σύγκριση με την επιλογή CTS2Self, επειδή η RTS/CTS περιλαμβάνει αναγνώριση από τη συσκευή λήψης. Για να χρησιμοποιήσετε την επιλογή RTS/CTS, διατηρήστε την προεπιλεγμένη ρύθμιση **RTS/CTS**. Η επιλογή None (Κανένα), ενδέχεται να προκαλέσει συγκρούσεις μεταξύ πακέτων OFDM και CCK. Για να χρησιμοποιήσετε την επιλογή None (Κανένα), επιλέξτε **None** (Κανένα). Για να χρησιμοποιήσετε την επιλογή CTS2Self, επιλέξτε **CTS2Self**.

11n Protection Type (Τύπος προστασίας 11n) Η επιλογή αυτή διαμορφώνει την προστασία από συσκευές χωρίς υψηλές ταχύτητες μεταγωγής εντός του ασύρματου δικτύου. Σε περίπτωση που ο ασύρματος δρομολογητής (ή σημείο πρόσβασης) εντοπίσει ένα συσχετισμό μιας παλαιάς συσκευής χωρίς υψηλές ταχύτητες μεταγωγής, θα δώσει σήμα σε όλες τις συσκευές με υψηλές ταχύτητες μεταγωγής να χρησιμοποιούν μηχανισμούς RTS/CTS ή CTS2Self πριν από κάθε μετάδοση δεδομένων. Η λειτουργία αυτή υποστηρίζει επίσης όλες τις τυπικές προστασίες 802.11n, συμπεριλαμβανομένης της MIMO.

Η επιλογή RTS/CTS παρέχει καλύτερη κάλυψη αλλά χαμηλότερες ταχύτητες μεταγωγής σε σύγκριση με την επιλογή CTS2Self, επειδή η RTS/CTS περιλαμβάνει αναγνώριση από τη συσκευή λήψης. Για να χρησιμοποιήσετε την επιλογή RTS/CTS, διατηρήστε την προεπιλεγμένη ρύθμιση **RTS/CTS**. Η επιλογή None (Κανένα), ενδέχεται να προκαλέσει συγκρούσεις μεταξύ πακέτων υψηλών ταχυτήτων μεταγωγής και παλαιών πακέτων. Για να χρησιμοποιήσετε την επιλογή None (Κανένα), επιλέξτε **None** (Κανένα). Για να χρησιμοποιήσετε την επιλογή CTS2Self, επιλέξτε **CTS2Self**.

Percentage of maximal transmit power (Ποσοστό μέγιστης ισχύος μετάδοσης) Η επιλογή αυτή ορίζει το ποσοστό μέγιστης ισχύος μετάδοσης σε σχέση με τους περιορισμούς ρυθμιστικού τομέα. Για παράδειγμα, εάν ο περιορισμός ρυθμιστικού τομέα επιτρέπει μεταδόσεις έως και 20 dB, η ρύθμιση του ποσοστού στο 50% επιτρέπει μέγιστη ισχύ μετάδοσης 10 dB. Επιλέξτε το ποσοστό που θέλετε να χρησιμοποιήσετε: **12%**, **25%**, **50%** ή **100%**. Η προεπιλεγμένη τιμή είναι **100%**.

QoS Classification Type (Τύπος κατηγοριοποίησης QoS) Η επιλογή αυτή ρυθμίζει αντιστοίχιση 802.1D ή 802.1Q από το πεδίο IP DSCP/TOS σε προτεραιότητες WMM (Background (Φόντο), Best Effects (Καλύτερη προσπάθεια), Video (Βίντεο), Voice (Φωνή)). Διατηρήστε την προεπιλογή **802.1D** ή επιλέξτε **802.1Q**, η οποία χρησιμοποιείται από ορισμένες ροές IPTV.

Re-establish Ethernet connection when initiating wireless connection (Επανεφαρμογή σύνδεσης Ethernet κατά την έναρξη ασύρματης σύνδεσης) Για την ενεργοποίηση εντοπισμού DHCP από τη συσκευή που βρίσκεται πίσω από τη γέφυρα, η γέφυρα θα πραγματοποιεί επαναφορά της σύνδεσης Ethernet ανάμεσα στη γέφυρα και τη συσκευή κάθε φορά που εφαρμόζεται ασύρματη σύνδεση. Για να απενεργοποιήσετε τη συμπεριφορά αυτή, επιλέξτε **No** (Όχι). Διαφορετικά, διατηρήστε την προεπιλεγμένη ρύθμιση **Yes** (Ναι).

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Administration (Διαχείριση) > Management (Διαχείριση λειτουργιών)

Χρησιμοποιήστε αυτήν την οθόνη για να διαχειριστείτε συγκεκριμένες λειτουργίες γέφυρας: πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα, δημιουργία αντιγράφου ασφαλείας του αρχείου διαμόρφωσης και επανεκκίνηση.



Management (Διαχείριση λειτουργιών)

Πρόσβαση στη γέφυρα

Χρησιμοποιήστε έναν κωδικό πρόσβασης για να προστατεύσετε την πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα.

Bridge Password (Κωδικός πρόσβασης γέφυρας) Εισαγάγετε ένα νέο κωδικό πρόσβασης για τη γέφυρα.

Re-Enter to Confirm (Επανεισαγωγή για επιβεβαίωση) Εισαγάγετε ξανά τον κωδικό πρόσβασης για να τον επιβεβαιώσετε.

Idle Timeout (Χρονικό όριο αδράνειας) Η σύνδεση λήγει μετά από την περίοδο αδράνειας που καθορίζετε. Το εύρος είναι **60** έως **3600** ms. Η προεπιλεγμένη τιμή είναι **600**.

Πρόσβαση στο Web

Access via Wireless (Πρόσβαση μέσω ασύρματης σύνδεσης) Εάν χρησιμοποιείτε τη γέφυρα σε δημόσιο τομέα από όπου παρέχετε ασύρματη πρόσβαση σε εξαρτημένους υπολογιστές, μπορείτε να απενεργοποιήσετε την ασύρματη πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα της γέφυρας. Εάν απενεργοποιήσετε τη λειτουργία αυτή, ο μόνος τρόπος να αποκτήσετε πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα θα είναι μέσω μιας ενσύρματης σύνδεσης. Διατηρήστε την προεπιλογή **Enabled** (Ενεργοποιημένη), για να επιτρέψετε την ασύρματη πρόσβαση στο διαδικτυακό βοηθητικό πρόγραμμα της γέφυρας ή επιλέξτε **Disabled** (Απενεργοποιημένη) για να εμποδίσετε την ασύρματη πρόσβαση στο βοηθητικό πρόγραμμα.

Δημιουργία αντιγράφου ασφαλείας και επαναφορά

Backup (Δημιουργία αντιγράφου ασφαλείας) Για να δημιουργήσετε αντίγραφο ασφαλείας του αρχείου διαμόρφωσης της γέφυρας, επιλέξτε **Backup Configurations** (Αντίγραφο ασφαλείας διαμορφώσεων). Στη συνέχεια, ακολουθήστε τις οδηγίες στην οθόνη.

Restore (Επαναφορά) Πατήστε **Browse** (Αναζήτηση) και επιλέξτε το αρχείο διαμόρφωσης. Έπειτα, πατήστε **Restore Configurations** (Επαναφορά διαμορφώσεων).

Επανεκκίνηση συστήματος

Reboot (Επανεκκίνηση) Για επανεκκίνηση της γέφυρας, επιλέξτε **Start to Reboot** (Έναρξη επανεκκίνησης).

Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων) για να ενεργοποιήσετε τις αλλαγές σας ή κάντε κλικ στην επιλογή **Cancel Changes** (Ακύρωση αλλαγών) για να ακυρώσετε τις αλλαγές σας.

Administration (Διαχείριση) > Factory Defaults (Εργοστασιακές ρυθμίσεις)

Χρησιμοποιήστε αυτήν την οθόνη για να επαναφέρετε τη διαμόρφωση της γέφυρας στις εργοστασιακά προεπιλεγμένες ρυθμίσεις.

Factory Defaults (Εργοστασιακές ρυθμίσεις)

Restore All Settings (Επαναφορά όλων των ρυθμίσεων) Για να επαναφέρετε τις εργοστασιακά προεπιλεγμένες ρυθμίσεις, πατήστε **Restore All Settings** (Επαναφορά όλων των ρυθμίσεων). Οι ρυθμίσεις που έχετε αποθηκεύσει θα χαθούν κατά την επαναφορά των προεπιλεγμένων ρυθμίσεων.



Administration (Διαχείριση) > Upgrade Firmware (Αναβάθμιση υλικολογισμικού)

Χρησιμοποιήστε αυτήν την οθόνη για αναβάθμιση του υλικολογισμικού της γέφυρας. Μην πραγματοποιήσετε αναβάθμιση του υλικολογισμικού εκτός αν αντιμετωπίζετε προβλήματα με τη γέφυρα ή εάν το νέο υλικολογισμικό διαθέτει κάποια λειτουργία που θέλετε να χρησιμοποιήσετε.



Πριν πραγματοποιήσετε αναβάθμιση του υλικολογισμικού, πραγματοποιήστε λήψη του αρχείου αναβάθμισης υλικολογισμικού της γέφυρας από τη διαδικτυακή τοποθεσία της Linksys, **www.Linksys.com/support**.

Upgrade Firmware (Αναβάθμιση υλικολογισμικού)

Please select a File to Upgrade (Επιλέξτε αρχείο για αναβάθμιση) Κάντε κλικ στο **Browse** (Αναζήτηση) και επιλέξτε το αρχείο αναβάθμισης υλικολογισμικού που έχετε εξαγάγει. Έπειτα, πατήστε **Start to Upgrade** (Έναρξη αναβάθμισης) και ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

Status (Κατάσταση) > Bridge (Γέφυρα)

Εμφανίζονται οι πληροφορίες τρέχουσας κατάστασης της γέφυρας.



Bridge Information (Πληροφορίες γέφυρας)

Firmware Version (Έκδοση υλικολογισμικού) Εμφανίζεται το τρέχον υλικολογισμικό της γέφυρας.

Local Network (Τοπικό δίκτυο)

Local MAC Address (Τοπική διεύθυνση MAC) Εμφανίζεται η διεύθυνση MAC της γέφυρας, όπως φαίνεται στο τοπικό σας δίκτυο Ethernet.

IP Address (Διεύθυνση IP) Εμφανίζεται η διεύθυνση IP της γέφυρας, όπως φαίνεται στο τοπικό σας δίκτυο Ethernet.

Subnet Mask (Μάσκα υποδικτύου) Εμφανίζεται η μάσκα υποδικτύου που έχει διαμορφωθεί για το τοπικό σας δίκτυο.

Status (Κατάσταση) > Wireless (Ασύρματη σύνδεση)

Εμφανίζονται πληροφορίες σχετικά με το ασύρματο δίκτυό σας.



Wireless (Ασύρματη σύνδεση)

Link Status (Κατάσταση σύνδεσης) Εμφανίζεται η κατάσταση της σύνδεσης στο ασύρματο δίκτυό σας.

MAC Address (Διεύθυνση MAC) Εμφανίζεται η διεύθυνση MAC της γέφυρας, όπως φαίνεται στο τοπικό σας ασύρματο δίκτυο.

Network Name (SSID) (Όνομα δικτύου (SSID)) Εμφανίζεται το όνομα του ασύρματου δικτύου/SSID.

BSSID Εμφανίζεται η διεύθυνση ασύρματου MAC του συνδεδεμένου ασύρματου δρομολογητή (ή σημείου πρόσβασης).

Radio Band (Ζώνη συχνοτήτων) Εμφανίζεται η ζώνη συχνοτήτων του ασύρματου δικτύου σας.

Channel Width (Πλάτος καναλιού) Εμφανίζεται το πλάτος καναλιού σε MHz, που χρησιμοποιείται από το ασύρματο δίκτυό σας.

Wide Channel (Ευρυζωνικό κανάλι) Ανάλογα με τις ρυθμίσεις καναλιού του δρομολογητή του δικτύου σας, εμφανίζεται η ρύθμιση Wide Channel (Ευρυζωνικό κανάλι). Εάν επιλέξατε Wide - 40MHz Channel (Ευρυζωνικό κανάλι 40MHz) για τη ρύθμιση Radio Band (Ζώνη συχνοτήτων) ή Channel Width (Πλάτος καναλιού) του δρομολογητή, αυτό θα είναι το πρωτεύον κανάλι για Wireless-N.

Standard Channel (Τυπικό κανάλι) Εμφανίζεται η ρύθμιση Standard Channel (Τυπικό κανάλι). Εάν επιλέξατε Wide – 40MHz Channel (Ευρυζωνικό κανάλι 40MHz) για τη ρύθμιση Radio Band (Ζώνη συχνοτήτων) ή Channel Width (Πλάτος καναλιού) του δρομολογητή, τότε το τυπικό κανάλι θα είναι το δευτερεύον κανάλι για Wireless-N.

Bit Rate (Ρυθμός bit) Εμφανίζεται ο ρυθμός μετάδοσης δεδομένων.

Signal (Σήμα) Εμφανίζεται το ποσοστό ισχύος του σήματος. Η ένδειξη 100% αντιστοιχεί στο ισχυρότερο δυνατό σήμα, ενώ η ένδειξη 0% στο πιο αδύναμο σήμα.

Security (Ασφάλεια) Εμφανίζεται η μέθοδος ασφάλειας που χρησιμοποιείται από το ασύρματο δίκτυό σας.

Αντιμετώπιση προβλημάτων

WES610N/WET610N

Ο υπολογιστής σας ή άλλη συσκευή ενσύρματης σύνδεσης Ethernet δεν μπορεί να επικοινωνήσει με τον ασύρματο δρομολογητή.

1. Προσπελάστε το διαδικτυακό βοηθητικό πρόγραμμα της γέφυρας.
2. Στην οθόνη *Basic Wireless Settings* (Βασικές ρυθμίσεις ασύρματης σύνδεσης), βεβαιωθείτε ότι το όνομα δικτύου (SSID) αντιστοιχεί στο όνομα του ασύρματου δικτύου σας.
3. Βεβαιωθείτε ότι οι ρυθμίσεις ασφάλειας (WPA, WPA2 ή WEP) αντιστοιχούν στις ρυθμίσεις ασφάλειας του ασύρματου δικτύου σας.

Η διεύθυνση IP της γέφυρας πρέπει να αλλαχθεί.

Εάν η γέφυρα είναι συνδεδεμένη σε ένα δίκτυο με ένα διακομιστή DHCP (συνήθως το δρομολογητή του δικτύου), θα λάβει τη διεύθυνση IP της από το διακομιστή DHCP. Εάν δεν υπάρχει διακομιστής DHCP, η γέφυρα θα χρησιμοποιήσει την προεπιλεγμένη στατική διεύθυνση IP της, **169.254.1.250**.

Εάν θέλετε η γέφυρα να χρησιμοποιεί πάντα μια στατική διεύθυνση IP, ακολουθήστε τις παρακάτω οδηγίες:

1. Προσπελάστε το διαδικτυακό βοηθητικό πρόγραμμα της γέφυρας.
2. Επιλέξτε την καρτέλα **Network Setup** (Ρυθμίσεις δικτύου).
3. Από το αναπτυσσόμενο μενού *Network Connection Type* (Τύπος σύνδεσης δικτύου), επιλέξτε **Static IP** (Στατική διεύθυνση IP).
4. Συμπληρώστε τα πεδία *Static IP Address* (Στατική διεύθυνση IP), *Subnet Mask* (Μάσκα υποδικτύου) και *Default Gateway* (Προεπιλεγμένη πύλη).
5. Κάντε κλικ στην επιλογή **Save Settings** (Αποθήκευση ρυθμίσεων).

Ο υπολογιστής ή άλλη συσκευή ενσύρματης σύνδεσης Ethernet δεν επικοινωνεί με συσκευές όπου έχει ενεργοποιηθεί ασύρματη σύνδεση (π.χ. υπολογιστή ή εκτυπωτή).

Ελέγξτε τα παρακάτω:

- Βεβαιωθείτε ότι η συσκευή με ενεργοποιημένη ασύρματη σύνδεση βρίσκεται στο ίδιο ασύρματο δίκτυο με τον υπολογιστή ή την άλλη συσκευή ενσύρματης σύνδεσης Ethernet που έχει συνδεθεί με τη θύρα.
- Βεβαιωθείτε ότι χρησιμοποιείται το ίδιο όνομα δικτύου (SSID) για όλες τις συσκευές στο ασύρματο δίκτυο.
- Βεβαιωθείτε ότι όλες οι συσκευές βρίσκονται στο ίδιο δίκτυο IP, χρησιμοποιώντας συμβατές διευθύνσεις IP.

Το διαδικτυακό βοηθητικό πρόγραμμα δεν εγκρίνει τον κωδικό πρόσβασης.

Ελέγξτε τα παρακάτω:

- Ο κωδικός πρόσβασης κάνει διάκριση πεζών-κεφαλαίων. Βεβαιωθείτε ότι χρησιμοποιείτε σωστά τα πεζά-κεφαλαία κατά την εισαγωγή του κωδικού πρόσβασης.
- Εάν ξεχάσετε τον κωδικό πρόσβασής σας, μπορείτε να επαναφέρετε τη γέφυρα στις εργοστασιακές προεπιλογές.

 Πατήστε παρατεταμένα το κουμπί **Reset** (Επαναφορά) της γέφυρας για περίπου πέντε δευτερόλεπτα. Ο κωδικός θα επανέλθει στην εργοστασιακή προεπιλογή, **admin**. Όλες οι άλλες ρυθμίσεις γέφυρας θα επιστρέψουν επίσης στις εργοστασιακές προεπιλογές. (Για να προσπελάσετε το διαδικτυακό βοηθητικό πρόγραμμα, πληκτρολογήστε **admin** στο πεδίο *Password* (Κωδικός πρόσβασης).)

Αφού εφαρμόσετε αλλαγές μέσω του διαδικτυακού βοηθητικού προγράμματος, οι νέες ρυθμίσεις δεν εμφανίζονται στην οθόνη.

Στο πρόγραμμα περιήγησης, επιλέξτε **Refresh** (Ανανέωση). Εάν δεν εμφανίζονται οι νέες ρυθμίσεις, ακολουθήστε τις εξής οδηγίες:

1. Αποσυνδέστε το καλώδιο τροφοδοσίας από τη γέφυρα.
2. Περιμένετε για πέντε δευτερόλεπτα και έπειτα επανασυνδέστε το καλώδιο τροφοδοσίας στη γέφυρα.
3. Στο πρόγραμμα περιήγησης, επιλέξτε **Refresh** (Ανανέωση).

WEB
Εάν εξακολουθείτε να έχετε απορίες, ανατρέξτε στη διαδικτυακή τοποθεσία της Linksys στη διεύθυνση **Linksys.com/support**

Προδιαγραφές

WES610N

Μοντέλο	WES610N
Πρότυπα	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Λυχνίες LED	Λειτουργίας, Ethernet, Wi-Fi Protected Setup™, Ασύρματης σύνδεσης, μεμονωμένης σύνδεσης Ethernet και δραστηριότητας
Θύρες	Ethernet (4), τροφοδοσίας
Κουμπιά	Επαναφοράς, Wi-Fi Protected Setup
Τύπος καλωδίωσης	CAT5e
Κεραίες	3 (εσωτερικές)
Τύπος υποδοχών κεραίας	Δ/Ι
Αποσπώμενο (Ναι/Όχι)	Όχι
Διαμορφώσεις	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Ισχύς ραδιοσυχνότητας (EIRP) σε dBm	802.11a: 15 dBm (τυπική) στα 54 Mbps 802.11b: 19 dBm (τυπική) στα 11 Mbps 802.11g: 16 dBm (τυπική) στα 54 Mbps 802.11n (2.4 GHz): 18 dBm (τυπική) στα MCS15 802.11n (5 GHz): 16 dBm (τυπική) στα MCS15
Ευαισθησία λήψης	802.11a: -72 dBm (τυπική) στα 54 Mbps 802.11b: -85 dBm (τυπική) στα 11 Mbps 802.11g: -73 dBm (τυπική) στα 54 Mbps 802.11n (20 MHz): -75 dBm (τυπική) στα MCS15 802.11n (40 MHz): -69 dBm (τυπική) στα MCS15
Απολαβή κεραίας σε dBi	1
Ασφάλεια ασύρματης σύνδεσης	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit κλειδιού ασφαλείας	Κρυπτογράφηση έως και 128 bit

Χαρακτηριστικά περιβάλλοντος λειτουργίας

Διαστάσεις	177 x 128 x 68 mm (6,97" x 5,04" x 2,68")
Βάρος	295 g (0,65 lb)
Πιστοποίηση	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Ισχύς	12V, 1A
Θερμοκρασία λειτουργίας	0 έως 40°C (32 έως 104°F)
Θερμοκρασία αποθήκευσης	-20 έως 60°C (-4 έως 140°F)
Υγρασία λειτουργίας	10% έως 85% χωρίς συμπύκνωση
Υγρασία αποθήκευσης	5% έως 90% χωρίς συμπύκνωση

Οι προδιαγραφές ενδέχεται να αλλάξουν χωρίς προειδοποίηση.

WET610N

Μοντέλο	WET610N
Πρότυπα	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Λυχνίες LED	Λειτουργίας, Ethernet, Wi-Fi Protected Setup™, Ασύρματης σύνδεσης
Θύρες	Ethernet, τροφοδοσίας
Κουμπιά	Επαναφοράς, Wi-Fi Protected Setup
Τύπος καλωδίωσης	CAT5e
Κεραίες	3 (εσωτερικές)
Τύπος υποδοχών κεραίας	Δ/Ι
Αποσπώμενο (Ναι/Όχι)	Όχι
Διαμορφώσεις	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Ισχύς ραδιοσυχνότητας (EIRP) σε dBm	802.11a: 15 dBm (τυπική) στα 54 Mbps 802.11b: 18 dBm (τυπική) στα 11 Mbps 802.11g: 16 dBm (τυπική) στα 54 Mbps 802.11n: 12 dBm (τυπική) στα 130 Mbps (HT20), 270 Mbps (HT40)
Ευαισθησία λήψης	802.11a: -72 dBm (τυπική) στα 54 Mbps 802.11b: -85 dBm (τυπική) στα 11 Mbps 802.11g: -73 dBm (τυπική) στα 54 Mbps 802.11n: -70 dBm (τυπική) στα MCS15/2.4 GHz, -69 dBm (τυπική) στα MCS15/5.0 GHz
Απολαβή κεραίας σε dBi	1
Ασφάλεια ασύρματης σύνδεσης	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit κλειδιού ασφαλείας	Κρυπτογράφηση έως και 128 bit

Χαρακτηριστικά περιβάλλοντος λειτουργίας

Διαστάσεις	145 x 106 x 52 mm (5,71" x 4,17" x 2,05")
Βάρος	159 g (5,61 oz)
Πιστοποίηση	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Ισχύς	12V, 1A
Θερμοκρασία λειτουργίας	0 έως 40°C (32 έως 104°F)
Θερμοκρασία αποθήκευσης	-20 έως 60°C (-4 έως 140°F)
Υγρασία λειτουργίας	10% έως 85% χωρίς συμπύκνωση
Υγρασία αποθήκευσης	5% έως 90% χωρίς συμπύκνωση

Οι προδιαγραφές ενδέχεται να αλλάξουν χωρίς προειδοποίηση.

Linksys.com/support

Η επωνυμία Cisco, το λογότυπο Cisco και η επωνυμία Linksys αποτελούν εμπορικά σήματα ή σήματα κατατεθέντα της Cisco ή/και των θυγατρικών της εταιρειών στις Ηνωμένες Πολιτείες Αμερικής και σε άλλες χώρες.
Μπορείτε να βρείτε τη λίστα εμπορικών σημάτων της Cisco στη διεύθυνση www.cisco.com/go/trademarks. Όλα τα υπόλοιπα εμπορικά σήματα που αναφέρονται στο παρόν έγγραφο αποτελούν ιδιοκτησία των αντίστοιχων κατόχων τους.

© 2011 Cisco ή/και θυγατρικές εταιρείες. Με την επιφύλαξη παντός δικαιώματος.

3425-01249



Felhasználói kézikönyv

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Tartalom

Termék-összefoglaló

LED panel 2
Portok panel 3

A vezeték nélküli hálózat biztonsága

A vezeték nélküli hálózat nevének (SSID) megváltoztatása 4
Saját jelszó beállítása 4
MAC címszűrés bekapcsolása 4
Titkosítás bekapcsolása 4

Általános hálózatbiztonsági alapelvek 4
További biztonsági tanácsok 5

Speciális beállítások

Hozzáférés a böngészőalapú segédprogramhoz. 6
Setup (Beállítás) > Basic Setup (Alapbeállítás) 7
Language (Nyelv) 7
Network Setup (Hálózat beállítása) 7

Wireless (Vezeték nélküli) > Basic Wireless Settings (Vezeték nélküli alapbeállítások) 7
Basic Wireless Settings (Vezeték nélküli alapbeállítások) 8
Wireless Security (Vezeték nélküli biztonság) 8
Wi-Fi Protected Setup (Wi-Fi védelmi beállítás) 9

Wireless (Vezeték nélküli) > Wireless Network Site Survey (Vezeték nélküli hálózat helyszín-feltérképezése) 10
Wireless Network Site Survey (Vezeték nélküli hálózat helyszín-feltérképezése) 10

Wireless > WMM® (Vezeték nélküli > WMM®) 11
WMM 12

Wireless (Vezeték nélküli) > Advanced Wireless Settings (Speciális beállítások) 13
Advanced Wireless (Speciális vezeték nélküli beállítások) 14

Administration (Felügyelet) > Management (Főfelügyelet) . . . 14
Management (Főfelügyelet) 14

Administration (Felügyelet) > Factory Defaults (Gyári alapbeállítások) 15
Factory Defaults (Gyári alapbeállítások) 15

Administration (Felügyelet) > Upgrade Firmware (Eszközszoftver frissítése) 15
Upgrade Firmware (Eszközszoftver frissítése) 15

Status (Állapot) > Bridge (Híd) 16
Bridge Information (Hídadatok) 16
Local Network (Helyi hálózat) 16

Status (Állapot) > Wireless (Vezeték nélküli). 16
Wireless (Vezeték nélküli) 16

Hibaelhárítás

WES610N/WET610N 17

Műszaki adatok

WES610N 18
WET610N 19

Termék-összefoglaló

Köszönjük, hogy a Linksys Dual-Band N Entertainment Bridge kétsávú szórakoztató hidat választotta. A híd képes bármilyen vezetékes Ethernet eszközt a vezeték nélküli hálózathoz kapcsolni. A híd kétsávú Wireless-N rendszerre épül, így kompatibilis bármelyik Wireless-N, -G, -A vagy -B útválasztóval vagy elérési ponttal. Az első telepítéshez kövesse a CD-lemez mappájában található lépéseket. A speciális beállításokat a kényelmesen használható, weblapként megjelenő segédprogram kezelőfelületén adhatja meg.

LED panel



WES610N WET610N

Vezeték nélküli (kék) A vezeték nélküli LED vezeték nélküli kapcsolat fennállásakor világít. A LED a híd által a vezeték nélküli hálózaton keresztül végzett adatküldési, illetve adatfogadási művelet közben villog.

Wi-Fi Protected Setup Button (Wi-Fi védelmi beállítás gomb) Ha az útválasztó támogatja a Wi-Fi védelmi beállítást, és WPA vagy WPA2 biztonsági eljárást használ, akkor a Wi-Fi Protected Setup (Wi-Fi védelmi beállítás) segítségével automatikusan csatlakozhat a hídhoz. A Wi-Fi védelmi beállítással kapcsolatos további információkat a következő helyen talál: „Wireless (Vezeték nélküli) > Basic Wireless Settings (Vezeték nélküli alapbeállítások)”, 7. oldal.

Wi-Fi Protected Setup (Wi-Fi védelmi beállítás) LED-je (kék/narancs) A LED két percen keresztül kéken villog a Wi-Fi Protected Setup (Wi-Fi védelmi beállítás) alatt. Kék fényt ad, amikor a vezeték nélküli átvitel védelme aktiválódott. Ha hiba történt a Wi-Fi Protected Setup (Wi-Fi védelmi beállítás) közben, a LED narancssárgán világít. Ellenőrizze, hogy a hálózati útválasztó Wi-Fi Protected Setup (WiFi védelmi beállítás) funkciót. Várja meg, míg a LED kialszik, majd próbálja újra.

Ethernet (kék) Az Ethernet LED vezetékes kapcsolat fennállásakor világít. A LED a híd által az Ethernet portokon keresztül végzett adatküldési, illetve adatfogadási művelet közben villog.

Power (Tápellátás) (kék) A tápellátás LED-je a híd bekapcsolásakor világít.

Portok panel



WES610N WET610N

Ethernet Az Ethernet portokon keresztül csatlakozik a híd a számítógéphez vagy más Ethernet hálózati eszközhöz. A WES610N típus négy porttal rendelkezik, a WET610N viszont csak eggyel.

Reset (Visszaállítás) Két módon lehet visszaállítani a híd gyári alapbeállításait. A Reset (Visszaállítás) gomb kb. 5 másodperces nyomva tartásával, valamint a híd böngészőalapú segédprogramjában az Administration (Felügyelet) > Factory Defaults (Gyári alapbeállítások) menüponton keresztül. A Reset (Visszaállítás) gomb a WES610N típusnak az alján, a WET610N típusnak pedig a hátsó portot tartalmazó panelján található.

Power (Tápellátás) A híd a tápellátás porton keresztül csatlakoztatható a mellékelt hálózati csatlakozóhoz.

A vezeték nélküli hálózat biztonsága

A vezeték nélküli hálózatokat kényelmesen és könnyen lehet telepíteni, ezért a nagy sebességű internetkapcsolattal rendelkező háztartásokban egyre gyakrabban alkalmazzák. A vezeték nélküli hálózat rádióhullámokkal továbbítja az adatokat, épp ezért a hagyományos vezetékes hálózatnál kiszolgáltatottabb a külső behatolással szemben. A vezeték nélküli hálózat jeleit is éppen úgy lehet fogni, akár a mobiltelefonok és vezeték nélküli készülékek adásait. Mivel fizikailag nem zárhatja ki, hogy valaki belépjen a vezeték nélküli hálózatába, ezért a hálózat biztonsága érdekében más lépéseket kell megtennie.

A vezeték nélküli hálózat nevének (SSID) megváltoztatása

A vezeték nélküli eszközöknek gyári alapbeállításban van egy hálózati nevük (SSID). Ez a maximum 32 karakterből álló sorozat a vezeték nélküli hálózat neve. A Linksys vezeték nélküli készülékekben a **linksys** szó van hálózati névként gyárilag beállítva. Ajánlatos a vezeték nélküli hálózatnak ezt a nevét megváltoztatni, és valamilyen egyedi névvel megkülönböztetni a hálózatát a környezetében található többi vezeték nélküli hálózattól. Erre ne használjon túl személyes információt (pl. tb-számot), mert ezt a nevet láthatják mások is, amikor megnézik az elérhető vezeték nélküli hálózatok listáját.

Saját jelszó beállítása

Vezeték nélküli készülékeknél (pl. hozzáférési pont és útválasztó) a beállítások megváltoztatásához jelszót kell megadnia. Az eszközöknek gyári alapbeállításban van egy jelszavuk. A Linksys gyári jelszava az **admin**. A jogosulatlan behatolók ismerik a gyári beállításokat, és megpróbálhatják megváltoztatni az Ön hálózatának beállításait. A jogosulatlan beavatkozások meghiúsítására változtassa olyanra az eszköz jelszavát, hogy azt nehéz legyen kitalálni.

MAC címszűrés bekapcsolása

A Linksys útválasztókban engedélyezni lehet az Eszközhozzáférést szabályozó (MAC) címek szűrését. A MAC-cím számokból és betűkből álló sorozat, amely gyakorlatilag minden egyes hálózati eszközben más és más. A MAC-címek szűrésének bekapcsolásával a vezeték nélküli hálózathoz csak megadott MAC-című eszközök csatlakozhatnak. Például megadhatja a háztartásában lévő számítógépek MAC-címét, hogy csak ezek csatlakozhassanak a vezeték nélküli hálózathoz.

Titkosítás bekapcsolása

A titkosítás megvédi a vezeték nélküli hálózaton küldött adatait. A Wi-Fi védett hozzáférés (WPA/WPA2) és a Vezetékessel egyenértékű adatvédelem (WEP) a vezeték nélküli adatátvitel biztonságát nem egyforma szinten biztosítja.

A WPA/WPA2 alkalmazásával titkosított hálózat biztonságosabb a WEP-nél, mert a WPA/WPA2 dinamikus kulcsú titkosítást használ. A rádióhullámok által továbbított adatok védelmére ajánlatos az eszközök által támogatott legmagasabb szintű titkosítást bekapcsolni.

A WEP régebbi titkosítási szabvány, de esetleg ezt kell választani olyan régebbi eszközök esetében, amelyek még nem támogatják a WPA-eljárást.

Általános hálózatbiztonsági alapelvek

A vezetékes hálózat biztosítása semmit sem ér, hogyha maga a hálózat nem biztonságos.

- Védjen jelszóval minden hálózati számítógépet, és külön jelszóval lásson el minden bizalmas fájlt.
- A jelszókat változtassa rendszeres időközönként.
- Telepítsen vírusirtó szoftvert és személyes tűzfalszoftvert.
- Kapcsolja ki az egyenrangú (peer-to-peer) fájlmegosztást. Egyes alkalmazások esetleg a tudta és/vagy beleegyezése nélkül bekapcsolják a fájlmegosztást.

További biztonsági tanácsok

- A vezeték nélküli útválasztókat, hozzáférési pontokat és átjárókat a kifelé néző falaktól és ablakoktól távolabb helyezze el.
- Tartsa kikapcsolva a vezeték nélküli útválasztókat, hozzáférési pontokat és átjárókat, amikor nincsenek használatban (éjjel, üdüléskor).
- Használjon erős jelmondatokat, amelyek legalább nyolc karakter hosszúságúak. Keverjen benne számokat és betűket, valamint kerülje a normál szótári szavak használatát.

Speciális beállítások

A CD-lemez mappájában található lépések szerint történő beállítása után a híd használatra kész. A böngészőalapú segédprogram segítségével azonban módosíthatja a híd speciális beállításait. Ez a fejezet tárgyalja a kezelőfelület egyes weblapjait és a lapokon elérhető alapvető fontosságú műveleteket. A segédprogram a híddal egy hálózatba kötött számítógép böngészőprogramján keresztül érhető el.

A böngészőalapú segédprogram ezekből a fő lapokból áll: Setup (Beállítás), Wireless (Vezeték nélküli), Administration (Felügyelet) és Status (Állapot). A fő lapokra kattintva további lapok közül választhat.

Hozzáférés a böngészőalapú segédprogramhoz

Használjon webböngészőt a böngészőalapú segédprogram eléréséhez.

Ha a híd DHCP-kiszolgálóval (ez rendszerint a hálózati útválasztó) kapcsolódik a hálózatra, akkor a híd a DHCP-kiszolgálótól kap IP-címet. Ha nincs DHCP-kiszolgáló, akkor a híd az alapértelmezett statikus IP-címét használja: **169.254.1.250**. (Amennyiben böngészőalapú segédprogramon keresztül állítja be a híd állandó statikus IP-címét, akkor inkább a statikus IP-címet adja meg helyette.)

MEGJEGYZÉS
Ha nem ismeri a híd IP-címét, akkor azt az útválasztó DHCP ügyféltáblázatából keresheti ki. (Ezt az útválasztó dokumentációjában találja.)

Ha nem találja meg a híd IP-címét, visszaállíthatja a hidat, ehhez egy kiegyenesített iratkapoccsal tartsa lenyomva a híd **Reset** (Visszaállítás) gombját. Ezzel visszaállítja a híd gyári alapbeállításait. A híd a DHCP-kiszolgálótól (ez rendszerint a hálózati útválasztó) kér IP-címet. Ha nem talál DHCP-kiszolgálót, akkor a híd a **169.254.1.250** alapértelmezett statikus IP-címét használja mindaddig, amíg meg nem találja a DHCP-kiszolgálót, és amíg nincs hozzárendelve egy dinamikus IP-cím.

Ha a híd nincs társítva egy útválasztóhoz, és a gyári alapbeállításokat használja, a web-alapú segédprogram eléréséhez Ethernet csatlakozáson keresztül csatlakoztassa a hidat egy számítógéphez. Konfigurálja a számítógépen az Ethernet csatlakozást egy statikus IP-címmel és alhálózati maszkkal.

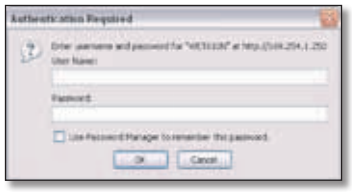
Az Ethernet adapter IP-címét egy megadott IP-címre kell beállítani.

1. Az *IP address* (IP-cím) mezőbe írja be az **169.254.x.y** értéket (x helyett egy 1 és 254 közötti számot, y helyett pedig egy 0 és 255 közötti számot kell megadni).
2. A *Subnet mask* (Alhálózati maszk) mezőbe írja be a **255.255.0.0** értéket.

MEGJEGYZÉS
A statikus IP-címnek a számítógépen az Ethernet adapterhez történő hozzárendeléséhez szükséges lépések operációs rendszerenként eltérők lehetnek. A vonatkozó utasításokat az adott operációs rendszer súgó dokumentációjában találja.

Miután hozzárendelte az Ethernet adaptert egy statikus IP-címhez, indítsa el a webböngészőt, és az *Address* (Cím) mezőben adja meg az adapter IP-címét (az alapértelmezett beállítás **169.254.1.250**). Nyomja meg az **Enter** billentyűt.

Ekkor megjelenik a jelszó megadására szolgáló képernyő. (A nem Windows XP operációs rendszert használóknak is hasonló képernyő jelenik meg.) Hagyja üresen a *User name* (Felhasználónév) mezőt. Adja meg a telepítővarázslóban generált jelszót. Ha nem hozott létre új jelszót, az alapértelmezés szerinti **admin** jelszót adja meg. A jelszót megváltoztathatja az *Administration* (Felügyelet) lap *Management* (Főfelügyelet) képernyőjén. Kattintson az **OK** gombra a folytatáshoz.



MEGJEGYZÉS
Ha nem jelenik meg a jelszó megadására szolgáló képernyő, várjon két percig, majd próbálja újra a műveletet.

Setup (Beállítás) > Basic Setup (Alapbeállítás)

Elsőként a *Basic Setup* (Alapbeállítás) képernyő jelenik meg. Ezen a képernyőn módosíthatja a böngészőalapú segédprogram nyelvét és a híd vezetékes, Ethernet hálózati beállításait.





Language (Nyelv)

Language (Nyelv) Itt adható meg a weblapként megjelenő kezelőfelület nyelve. Válassza ki a kívánt nyelvet a legördülő listából.

Network Setup (Hálózat beállítása)

Ebben a részben adható meg, hogy automatikusan a DHCP-kiszolgálótól (pl. a hálózati útválasztótól) kapjon-e IP-címet a híd, vagy manuálisan kívánja-e azt beállítani. Az első esetben az Automatic Configuration (Automatikus konfiguráció) - DHCP lehetőséget, az utóbbiban pedig a Static IP (Statikus IP-cím) lehetőséget kell választani.

Bridge IP (Híd IP-címe) Ha a hálózatban van a hálózati eszközöknek IP-címet kiosztó DHCP-kiszolgáló (pl. hálózati útválasztó), hagyja meg az alapértelmezett **Automatic Configuration - DHCP** (Automatikus konfiguráció - DHCP) beállítást. A híd a DHCP-kiszolgálótól (ez rendszerint a hálózati útválasztó) kér IP-címet. Ha nem talál DHCP-kiszolgálót, akkor a híd a **169.254.1.250** alapértelmezett statikus IP-címét használja mindaddig, amíg meg nem találja a DHCP-kiszolgálót, és amíg nincs hozzárendelve egy dinamikus IP-cím.

Ha állandó statikus IP-címet szeretne megadni a híd számára, válassza a **Static IP** (Statikus IP-cím) lehetőséget.

Ha a Static IP (Statikus IP-cím) lehetőséget választja, adja meg következő mezők értékét:

- **Static IP Address** (Statikus IP-cím) Itt adhatja meg a weblapként megjelenő kezelőfelület megnyitására szolgáló egyedi IP-címet.
- **Subnet Mask** (Alhálózati maszk) Itt adhatja meg a vezetékes hálózat alhálózati maszkját.
- **Default Gateway** (Alapértelmezett átjáró) Itt adhatja meg a hálózat alapértelmezett átjárójának (ez általában az útválasztó) IP-címét:

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Wireless (Vezeték nélküli) > Basic Wireless Settings (Vezeték nélküli alapbeállítások)

A *Basic Wireless Settings* (Vezeték nélküli alapbeállítások) képernyőn adhatja meg a híd vezeték nélküli és biztonsági alapbeállításait.

A híd beállításai kétféleképpen, kézileg és a Wi-Fi védelmi beállítással (Wi-Fi Protected Setup) konfigurálhatók. A Wi-Fi védelmi beállítás olyan szolgáltatás, amellyel a vezeték nélküli hálózat könnyen beállítható. Ha a hálózati útválasztó támogatja a Wi-Fi védelmi beállítást és WPA vagy WPA2 biztonsági megoldást használ, akkor a Wi-Fi védelmi beállítás segítségével automatikusan csatlakozhat a hídhoz.

Configuration View (Konfigurációs nézet) A vezeték nélküli hálózat kézi beállításához válassza a **Manual** (Kézi) lehetőséget. Olvassa el: **Basic Wireless Settings** (Vezeték nélküli alapbeállítások), **8. oldal**. Ha Wi-Fi védelmi telepítést kíván használni, akkor válassza a **Wi-Fi Protected Setup** (Wi-Fi védelmi telepítés) lehetőséget. Olvassa el: **Wi-Fi Protected Setup** (Wi-Fi védelmi beállítás), **9. oldal**.

Basic Wireless Settings (Vezeték nélküli alapbeállítások)



Network Name, SSID (Hálózati név, SSID) Az SSID hálózati név, amely egyaránt érvényes a vezeték nélküli hálózat minden pontján. Az SSID névnek a hálózat valamennyi eszközén azonosnak kell lennie. A névben különbözőnek számítanak a kis- és a nagybetűk, a név legfeljebb 32 karakter hosszúságú lehet (a billentyűzet bármely karaktere használható). Győződjön meg róla, hogy a beállítás megegyezik a vezeték nélküli útválasztó vagy a hozzáférési pont beállításával. A biztonság fokozására ajánlatos az alapbeállítás szerinti SSID nevet (**linksys**) egy másik névre cserélni.

Wireless Security (Vezeték nélküli biztonság)

A híd a következő vezeték nélküli biztonsági lehetőségeket támogatja: WPA Personal, WPA2 Personal és WEP. A WPA (Wi-Fi védett hozzáférés) és a WPA2 erősebb védelmi eljárás, mint a WEP (vezetékessel egyenértékű adatvédelem). A vezeték nélküli biztonsággal kapcsolatos további tudnivalók: „A vezeték nélküli hálózat biztonsága”, 4. oldal.

Security Mode (Biztonsági üzemmód)

Válasszon a hálózatának biztonsági üzemmódot. Ha nem kíván semmilyen titkosítási eljárást használni, akkor hagyja az alapbeállítás szerinti **Disabled** (Kikapcsolt) állapotban.

MEGJEGYZÉS
Ügyeljen arra, hogy a vezeték nélküli hálózat minden egyes eszközének egyforma biztonsági eljárást és jelmondatot/kulcsot használjon különben nem fognak tudni kommunikálni egymással a vezeték nélküli eszközök.

WPA Personal (WPA személyi)

A WPA a WEP-titkosításnál hatásosabb biztonsági szabvány.



Encryption (Titkosítás) A WPA a dinamikus titkosítási kulcsú TKIP titkosítási eljárást támogatja.

Passphrase (Jelmondat) Adja meg a híd és a vezeték nélküli útválasztó vagy hozzáférési pont közös kódkulcsát. 8-63 karakter hosszúnak kell lennie.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

WPA2 Personal (WPA2 személyi)

A WPA2 a WPA tovább fejlesztett, biztonságosabb változata.



Encryption (Titkosítás) A WPA2 két titkosítási eljárást, a TKIP és AES dinamikus titkosítási kulcsú eljárást támogatja. Válassza ki a használni kívánt titkosítási eljárást: **AES** vagy **TKIP or AES**. Az alapbeállítás **AES**.

Passphrase (Jelmondat) Adja meg a híd és a vezeték nélküli útválasztó vagy hozzáférési pont közös kódkulcsát. 8-63 karakter hosszúnak kell lennie.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

WEP

A WEP a WPA-nál és a WPA2-nél kevésbé biztonságos, egyszerű titkosítási eljárás.



Encryption (Titkosítás) Válassza meg a WEP titkosítási szintjét **40/64 bit (10 hexadecimális számjegy)** vagy **104/128 bit (26 hexadecimális számjegy)**. Az alapbeállítás **40/64 bit (10 hexadecimális számjegy)**.

Key 1 (1. kulcs) Adja meg a hálózat WEP-kulcsát.

Tx Key (Tx kulcs): A **Key 1** (1. kulcs) a híd által használt átviteli kulcs.

Authentication (Hitelesítés) Alapbeállítás szerint **Auto** (Automatikus), és így mind Open System (Nyílt rendszerű), mind Shared Key (Megosztott kulcsú) hitelesítés használható. Az **Open** (Nyílt) lehetőséget kiválasztva használhatja a nyílt rendszerű hitelesítést, amikor a feladó és a címzett nem használ WEP-kódkulcsot a hitelesítéshez. A **Shared** (Megosztott) lehetőséget kiválasztva használhatja a megosztott kulcsú hitelesítést, amikor a feladó és a címzett használ WEP-kódkulcsot a hitelesítéshez.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Wi-Fi Protected Setup (Wi-Fi védelmi beállítás)

Két módszer lehetséges. Azt a módszert válassza, amelyik megfelel a használt útválasztónak.





1. módszer

Akkor alkalmazza ezt a módszert, ha az útválasztón van Wi-Fi védelmi beállítás gomb.

1. Nyomja meg a **Wi-Fi Protected Setup** (Wi-Fi védelmi beállítás) gombot az útválasztón.
2. Két percen belül kattintson a **Wi-Fi Protected Setup** (Wi-Fi védelmi beállítás) gombra a híd *Wi-Fi Protected Setup* (Wi-Fi védelmi beállítás) képernyőjén.
3. A híd konfigurálása után kattintson a **Close** (Bezárás) gombra.

A *Wi-Fi Protected Setup* (Wi-Fi védelmi beállítás) képernyőn megjelenik a Link Status (Hivatkozás állapota), a Network Name (SSID)(Hálózati név (SSID)) és a Security method (Biztonsági eljárás).

2. módszer

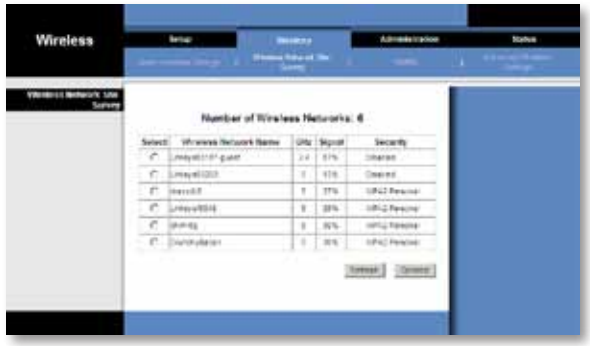
Ezt a módszert akkor alkalmazza, ha az útválasztó kéri a híd PIN-kódját.

1. Az **útválasztó** *Wi-Fi Protected Setup* (Wi-Fi védelmi beállítás) képernyőjén adja meg a **híd** *Wi-Fi Protected Setup* (Wi-Fi védelmi beállítás) képernyőjén megjelenő PIN-kódot. Kattintson a **Register** (Regisztráció) vagy az ennek megfelelő gombra. (A híd hátlapján lévő címkén is szerepel.)
2. A **híd** *Wi-Fi Protected Setup* (Wi-Fi védelmi beállítás) képernyőjén kattintson az **OK** gombra.
3. A híd konfigurálása után kattintson a **Close** (Bezárás) gombra.

A *Wi-Fi Protected Setup* (Wi-Fi védelmi beállítás) képernyőn megjelenik a Link Status (Hivatkozás állapota), a Network Name (SSID)(Hálózati név (SSID)) és a Security method (Biztonsági eljárás).

Wireless (Vezeték nélküli) > Wireless Network Site Survey (Vezeték nélküli hálózat helyszín-feltérképezése)

A helyszín-feltérképezés megkezdéséhez kattintson a **Wireless Network Site Survey** (Vezeték nélküli hálózat helyszín-feltérképezése) fülre. A *Wireless Network Site Survey* (Vezeték nélküli hálózat helyszín-feltérképezése) képernyőn megjelenik a híd által érzékelt vezeték nélküli hálózatok listája.



Wireless Network Site Survey (Vezeték nélküli hálózat helyszín-feltérképezése)

Number of Wireless Networks (Vezeték nélküli hálózatok száma) Itt látható a híd által érzékelt vezeték nélküli hálózatok száma.

Select (Kiválasztás) Egy vezeték nélküli hálózathoz történő csatlakozáshoz kattintson a **Select** (Kiválasztás) gombra. Aztán kattintson a **Connect** (Csatlakozás) gombra.

Wireless Network Name (Vezeték nélküli hálózat neve) Itt látható a vezeték nélküli hálózat hálózatneve (vagy SSID).

GHz Itt látható a vezeték nélküli hálózat rádiósávja.

Signal (Jel) Itt látható a jelerősség százalékban kifejezett értéke. 100% a lehető legnagyobb jelerősséget, 0% pedig a lehető legkisebb jelerősséget jelöli.

Security (Biztonság) Ha a hálózat támogatja a Wi-Fi védelmi beállítást, akkor megjelenik a Wi-Fi Protected Setup (Wi-Fi védelmi beállítás) ikonja. Itt látható a vezeték nélküli hálózat által használt biztonsági eljárás.

A képernyőn látható adatokat a **Refresh** (Frissítés) gombbal aktualizálhatja.

Miután kiválasztott egy hálózatot, kattintson a **Connect** (Csatlakozás) gombra. Ekkor új képernyő jelenik meg. Kövesse a hálózat biztonsági eljárására vonatkozó utasításokat.

WPA



Network Name (SSID) (Hálózatnév (SSID)) Automatikusan megjelenik a kiválasztott hálózat neve.

Security Mode (Biztonsági üzemmód) Automatikusan megjelenik a WPA Personal (WPA személyi).

Encryption (Titkosítás) A WPA a dinamikus titkosítási kulcsú TKIP titkosítási eljárást támogatja.

Passphrase (Jelmondat) Adja meg a híd és a vezeték nélküli útválasztó vagy hozzáférési pont közös kódkulcsát. 8-63 karakter hosszúnak kell lennie.

A képernyőn látható adatokat a **Refresh** (Frissítés) gombbal aktualizálhatja.

Miután megadta a biztonsági beállításokat, kattintson a **Connect** (Csatlakozás) gombra.

WPA2



Network Name (SSID) (Hálózatnév (SSID)) Automatikusan megjelenik a kiválasztott hálózat neve.

Security Mode (Biztonsági üzemmód) Automatikusan megjelenik a WPA2 Personal (WPA2 személyi).

Encryption (Titkosítás) A WPA2 két titkosítási eljárást, a TKIP és AES dinamikus titkosítási kulcsú eljárást támogatja. Válassza ki a használni kívánt titkosítási eljárást: **AES** vagy **TKIP or AES**.

Passphrase (Jelmondat) Adja meg a híd és a vezeték nélküli útválasztó vagy hozzáférési pont közös kódkulcsát. 8-63 karakter hosszúnak kell lennie.

A képernyőn látható adatokat a **Refresh** (Frissítés) gombbal aktualizálhatja.

Miután megadta a biztonsági beállításokat, kattintson a **Connect** (Csatlakozás) gombra.

WEP



Network Name (SSID) (Hálózatnév (SSID)) Automatikusan megjelenik a kiválasztott hálózat neve.

Security Mode (Biztonsági üzemmód) Automatikusan megjelenik a WEP.

Encryption (Titkosítás) Válassza ki a WEP titkosítási szintjét **40/64 bit (10 hexadecimális számjegy)** vagy **104/128 bit (26 hexadecimális számjegy)**.

Key 1 (1. kulcs) Adja meg a hálózat WEP-kulcsát.

Tx Key (Tx kulcs): A **Key 1** (1. kulcs) a híd által használt átviteli kulcs.

Authentication (Hitelesítés) Alapbeállítás szerint **Auto** (Automatikus), és így mind Open System (Nyílt rendszerű), mind Shared Key (Megosztott kulcsú) hitelesítés használható. Az **Open** (Nyílt) lehetőséget kiválasztva használhatja a nyílt rendszerű hitelesítést, amikor a feladó és a címzett nem használ WEP-kódkulcsot a hitelesítéshez. A **Shared** (Megosztott) lehetőséget kiválasztva használhatja a megosztott kulcsú hitelesítést, amikor a feladó és a címzett használ WEP-kódkulcsot a hitelesítéshez.

A képernyőn látható adatokat a **Refresh** (Frissítés) gombbal aktualizálhatja.

Miután megadta a biztonsági beállításokat, kattintson a **Connect** (Csatlakozás) gombra.

Wireless > WMM® (Vezeték nélküli > WMM®)

Itt konfigurálhatja a vezeték nélküli MultiMedia (WMM) beállításokat. A WMM hozzáférési módjaiknak (forgalmi típusuknak) megfelelően rangsorolja a csomagokat: Background (Háttér), Best Effort (Legjobb lehetőség), Video (Videó) vagy Voice (Hang). Ezek beállításait megváltoztatni csak gyakorlott rendszergazdák számára ajánlott, mert a helytelen beállítás csökkentheti a hálózat teljesítményét.



MEGJEGYZÉS
A *WMM* képernyőn látható beállításokat csak kellő ismerettel rendelkező felhasználóknak célszerű megváltoztatni.

WMM

Access Mode (Hozzáférési mód)

Különböző beállításokat rendelhet a négy rendelkezésre álló hozzáférési módhoz. Válassza ki a konfigurálni kívánt módot: **Background** (Háttér), **Best Effort** (Legjobb lehetőség), **Video** (Videó) vagy **Voice** (Hang). Hajtsa végre a választott módra vonatkozó utasításokat.

Background (Háttér)

Use Aggregation (Halmozás alkalmazása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg kialakítson-e blokknyugtázást hozzáadó (ADDBA) munkamenetet. Az alapbeállítás **No** (Nem). A lehetőség engedélyezéséhez válassza a **Yes** (Igen) értéket.

Accept Aggregation (Halmozás elfogadása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg fogadja-e az ADDBA-kérelmeket. Az alapbeállítás **Yes** (Igen). A működés deaktiválásához válassza a **No** (Nem) lehetőséget.

Max. Number of Packets in Aggregation (Halmozható csomagok max. száma) Ez a beállítás határozza meg a halmozható csomagok (alkeretek) maximális számát. A rendelkezésre álló tartomány **0**–**7**. Alapértéke **7**.

Max. Aggregation Size (Max. halmozható méret) Ez a beállítás határozza meg a halom maximális méretét (bájtban). A rendelkezésre álló tartomány **0**–**16 000**. Alapértéke **12 000**.

Timeout Interval (Időtúllépés időköze) Ez a beállítás határozza meg azt az időszakot, amelynek elteltével a halmot egy „záró feltétel" alapján le kell zárni, mielőtt azt az időzítő lezárná. A rendelkezésre álló tartomány **0**–**100** ms. Alapértéke **3**.

Min. Size of Packet in Aggregation (Halmozható csomagok min. mérete) Ez a beállítás határozza meg a halmozható csomagok minimális méretét (bájtban). A rendelkezésre álló tartomány **0**–**1500**. Alapértéke **10**.

ADDBA Timeout (ADDBA időtúllépés) Ez a beállítás határozza meg azt az időtartamot, amelynek elteltével az ADDBA-beállítást le kell állítani abban az esetben, ha az adott időtartam alatt nem zajlik keretforgalom a blokknyugtázási (ACK) egyeztetés során. A rendelkezésre álló tartomány **0**–**65 535** ms. Alapértéke **0**, ez letiltja az időkorlátot.

Aggregation Window Size (Halmozóablak mérete) Ez a beállítás határozza meg az ACK-nyugtázás nélkül átvihető csomagok maximális számát. A rendelkezésre álló tartomány **0**–**64**. Alapértéke **64**.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Legjobb lehetőség

Use Aggregation (Halmozás alkalmazása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg kialakítson-e blokknyugtázást hozzáadó (ADDBA) munkamenetet. Az alapbeállítás **Yes** (Igen). A működés deaktiválásához válassza a **No** (Nem) lehetőséget.

Accept Aggregation (Halmozás elfogadása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg fogadja-e az ADDBA-kérelmeket. Az alapbeállítás **Yes** (Igen). A működés deaktiválásához válassza a **No** (Nem) lehetőséget.

Max. Number of Packets in Aggregation (Halmozható csomagok max. száma) Ez a beállítás határozza meg a halmozható csomagok (alkeretek) maximális számát. A rendelkezésre álló tartomány **0**–**10**. Alapértéke **10**.

Max. Aggregation Size (Max. halmozható méret) Ez a beállítás határozza meg a halom maximális méretét (bájtban). A rendelkezésre álló tartomány **0**–**20 000**. Alapértéke **16 000**.

Timeout Interval (Időtúllépés időköze) Ez a beállítás határozza meg azt az időszakot, amelynek elteltével a halmot egy „záró feltétel" alapján le kell zárni, mielőtt azt az időzítő lezárná. A rendelkezésre álló tartomány **0**–**100** ms. Alapértéke **3**.

Min. Size of Packet in Aggregation (Halmozható csomagok min. mérete) Ez a beállítás határozza meg a halmozható csomagok minimális méretét (bájtban). A rendelkezésre álló tartomány **0**–**1500**. Alapértéke **10**.

ADDBA Timeout (ADDBA időtúllépés) Ez a beállítás határozza meg azt az időtartamot, amelynek elteltével az ADDBA-beállítást le kell állítani abban az esetben, ha az adott időtartam alatt nem zajlik keretforgalom a blokknyugtázási (ACK) egyeztetés során. A rendelkezésre álló tartomány **0**–**65 535** ms. Alapértéke **0**, ez letiltja az időkorlátot.

Aggregation Window Size (Halmozóablak mérete) Ez a beállítás határozza meg az ACK-nyugtázás nélkül átvihető csomagok maximális számát. A rendelkezésre álló tartomány **0**–**64**. Alapértéke **64**.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Video (Videó)

Use Aggregation (Halmozás alkalmazása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg kialakítson-e blokknyugtázást hozzáadó (ADDBA) munkamenetet. Az alapbeállítás **Yes** (Igen). A működés deaktiválásához válassza a **No** (Nem) lehetőséget.

Accept Aggregation (Halmozás elfogadása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg fogadja-e az ADDBA-kérelmeket. Az alapbeállítás **Yes** (Igen). A működés deaktiválásához válassza a **No** (Nem) lehetőséget.

Max. Number of Packets in Aggregation (Halmozható csomagok max. száma) Ez a beállítás határozza meg a halmozható csomagok (alkeretek) maximális számát. A rendelkezésre álló tartomány **0**–**7**. Alapértéke **7**.

Max. Aggregation Size (Max. halmozható méret) Ez a beállítás határozza meg a halom maximális méretét (bájtban). A rendelkezésre álló tartomány **0**–**16 000**. Alapértéke **12 000**.

Timeout Interval (Időtúllépés időköze) Ez a beállítás határozza meg azt az időszakot, amelynek elteltével a halmot egy „záró feltétel" alapján le kell zárni, mielőtt azt az időzítő lezárná. A rendelkezésre álló tartomány **0**–**100** ms. Alapértéke **3**.

Min. Size of Packet in Aggregation (Halmozható csomagok min. mérete) Ez a beállítás határozza meg a halmozható csomagok minimális méretét (bájtban). A rendelkezésre álló tartomány **0**–**1500**. Alapértéke **10**.

ADDBA Timeout (ADDBA időtúllépés) Ez a beállítás határozza meg azt az időtartamot, amelynek elteltével az ADDBA-beállítást le kell állítani abban az esetben, ha az adott időtartam alatt nem zajlik keretforgalom a blokknyugtázási (ACK) egyeztetés során. A rendelkezésre álló tartomány **0**–**65535** ms. Alapértéke **0**, ez letiltja az időkorlátot.

Aggregation Window Size (Halmozóablak mérete) Ez a beállítás határozza meg az ACK-nyugtázás nélkül átvihető csomagok maximális számát. A rendelkezésre álló tartomány **0**–**64**. Alapértéke **64**.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Voice (Hang)

Use Aggregation (Halmozás alkalmazása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg kialakítson-e blokknyugtázást hozzáadó (ADDBA) munkamenetet. Az alapbeállítás **Yes** (Igen). A működés deaktiválásához válassza a **No** (Nem) lehetőséget.

Accept Aggregation (Halmozás elfogadása) Ezzel a beállítással határozható meg, hogy a közegelérést vezérlő (MAC) réteg fogadja-e az ADDBA-kérelmeket. Az alapbeállítás **Yes** (Igen). A működés deaktiválásához válassza a **No** (Nem) lehetőséget.

Max. Number of Packets in Aggregation (Halmozható csomagok max. száma) Ez a beállítás határozza meg a halmozható csomagok (alkeretek) maximális számát. A rendelkezésre álló tartomány **0**–**2**. Alapértéke **2**.

Max. Aggregation Size (Max. halmozható méret) Ez a beállítás határozza meg a halom maximális méretét (bájtban). A rendelkezésre álló tartomány **0**–**16 000**. Alapértéke **10 000**.

Timeout Interval (Időtúllépés időköze) Ez a beállítás határozza meg azt az időszakot, amelynek elteltével a halmot egy „záró feltétel" alapján le kell zárni, mielőtt azt az időzítő lezárná. A rendelkezésre álló tartomány **0**–**100** ms. Alapértéke **10**.

Min. Size of Packet in Aggregation (Halmozható csomagok min. mérete) Ez a beállítás határozza meg a halmozható csomagok minimális méretét (bájtban). A rendelkezésre álló tartomány **0**–**1500**. Alapértéke **10**.

ADDBA Timeout (ADDBA időtúllépés) Ez a beállítás határozza meg azt az időtartamot, amelynek elteltével az ADDBA-beállítást le kell állítani abban az esetben, ha az adott időtartam alatt nem zajlik keretforgalom a blokknyugtázási (ACK) egyeztetés során. A rendelkezésre álló tartomány **0**–**65535** ms. Alapértéke **0**, ez letiltja az időkorlátot.

Aggregation Window Size (Halmozóablak mérete) Ez a beállítás határozza meg az ACK-nyugtázás nélkül átvihető csomagok maximális számát. A rendelkezésre álló tartomány **0**–**64**. Alapértéke **64**.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Wireless (Vezeték nélküli) > Advanced Wireless Settings (Speciális beállítások)

Adja meg a híd speciális vezeték nélküli beállításait. Ezek beállításait megváltoztatni csak gyakorlott rendszergazdák számára ajánlott, mert a helytelen beállítás csökkentheti a hálózat teljesítményét.



MEGJEGYZÉS
Az *Advanced Wireless Settings* (Speciális vezeték nélküli beállítások) képernyőn látható beállításokat csak kellő ismerettel rendelkező felhasználóknak célszerű megváltoztatni.

Advanced Wireless (Speciális vezeték nélküli beállítások)

Use LDPC (LDCP használata) A Low-Density Parity-Check Code (Alacsony sűrűségű paritás ellenőrző kód) (LDPC) engedélyezi vagy letiltja a hibajavítást az adatvesztés valószínűségének csökkentése érdekében a zajos csatornákban. A Rate Adaptation (Sebesség adaptációs) algoritmus automatikusan letiltja az LDPC-kódolást magas PHY működési sebesség (több, mint 162) esetén. A speciális LDCP hibajavító séma használatához tartsa meg a **Yes** (Igen) alapbeállítást. Ellenkező esetben válassza a **No** (Nem) értéket.

ERP Protection Type (ERP védelemtípus) Ez a beállítás az OFDM csomagok védelmét konfigurálja, annak ellenére, hogy a vezeték nélküli hálózaton belül 802.11b típusú állomások is jelen vannak. A híd RTS/CTS vagy CTS2Self csomagok 802.11b sebességosztályban való küldésével tájékoztatja a vezeték nélküli hálózatot, hogy OFDM csomagok átvitele következik, és megvédi a csomagokat a vezeték nélküli hálózaton. Az RTS/CTS és CTS2Self csomagok túlterhelést okoznak, ami alacsonyabb adatátviteli teljesítményt eredményezhet.

Az RTS/CTS beállítás jobb lefedettséget, de alacsonyabb átviteli sebességet biztosít, mint a CTS2Self, mert az RTS/CTS beállítás a fogadó eszköztől kapott nyugtázást tartalmaz. Az RTS/CTS beállítás használatához tartsa meg az **RTS/CTS** alapbeállítást. A None (Nem) beállítás az OFDM és CCK csomagok ütközéséhez vezethet. A None (Nem) beállítás használatához válassza a **None** (Nem) értéket. A CTS2Self beállítás használatához válassza a **CTS2Self** értéket.

11n Protection Type (11n Védelemtípus) Ez a beállítás a non-High Throughput (HT) (alacsony átviteli teljesítményű) eszközök védelmét konfigurálja a vezeték nélküli hálózaton belül. Abban az esetben, ha a vezeték nélküli útválasztó (vagy hozzáférési pont) non-HT hagyományos eszköz kapcsolódását érzékeli, jelezni fogja minden HT eszköznek, hogy minden adattovábbítás előtt használja az RTS/CTS vagy CTS2Self mechanizmust. Ez a szolgáltatás támogat minden 802.11n szabványos védelmet, beleértve a MIMO technológiát is.

Az RTS/CTS beállítás jobb lefedettséget, de alacsonyabb átviteli sebességet biztosít, mint a CTS2Self, mert az RTS/CTS beállítás a fogadó eszköztől kapott nyugtázást tartalmaz. Az RTS/CTS beállítás használatához tartsa meg az **RTS/CTS** alapbeállítást. A None (Nem) beállítás a HT és a hagyományos csomagok ütközéséhez vezethet. A None (Nem) beállítás használatához válassza a **None** (Nem) értéket. A CTS2Self beállítás használatához válassza a **CTS2Self** értéket.

Percentage of maximal transmit power (Maximális átviteli teljesítmény százaléka) Ez a beállítás a szabályozási tartományban érvényes korlátozásokhoz képest a maximális átviteli teljesítmény százalékát adja meg. Ha például a szabályozási tartományban érvényes korlátozás legfeljebb –20 dB átvitelre ad módot, akkor a az 50%-os százalékos érték megadása 10 dB maximális átviteli teljesítményt engedélyez. Válassza ki a használni kívánt százalékot: **12%**, **25%**, **50%** vagy **100%**. Alapértéke **100%**.

QoS Classification Type (Szolgáltatásminőség osztályozási típus) Ez a beállítás beállítja a 802.1D vagy 802.1Q protokollt, és hozzárendeli az IP csomagok DSCP/TOS mezőjéhez a WMM prioritásokat (Background (Háttér), Best Effects (Legjobb hatás), Video (Videó) vagy Voice (Hang)). Tartsa meg a **802.1D** alapbeállítást vagy válassza a bizonyos IPTV közvetítéseknél használt **802.1Q** beállítást.

Az Ethernet csatlakozás helyreállítása a vezeték nélküli hálózat inicializálásakor A DHCP feltérképezés indításához a híd mögött található eszközről a híd visszaállítja alaphelyzetbe az Ethernet kapcsolatot a híd és az eszköz között, valahányszor egy vezeték nélküli kapcsolat létrejön. A viselkedés letiltásához válassza a **No** (Nem) értéket. Egyébként hagyja meg az alapbeállítás szerinti **Yes** (Igen) értéket.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Administration (Felügyelet) > Management (Főfelügyelet)

Ezen a képernyőn felügyelheti a híd adott funkcióit: a web-alapú segédprogram elérése, biztonsági mentés készítése a konfigurációs fájlról, újraindítás.



Management (Főfelügyelet)

Bridge Access (A híd elérése)

Jelszóval védje a böngészőalapú segédprogramot jogosulatlan hozzáférés ellen.

Bridge Password (Híd jelszava) Adja meg a híd új jelszavát.

Re-enter to confirm (Jóváhagyás) Jóváhagyásként adja meg ismét a jelszót.

Idle Timeout (Üresjárat időtúllépése) A bejelentkezés érvényessége az itt megadott üresjárati időtartam után jár le. A rendelkezésre álló tartomány **60**–**3600** másodperc. Alapértéke **600**.

Web Access (Webhozzáférés)

Access via Wireless (Vezeték nélküli hozzáférés) Ha a hidat nyilvános tartományban használja, tehát külsősöknek is ad vezeték nélküli hozzáférést, akkor letilthatja a vezeték nélküli hozzáférést a híd böngészőalapú segédprogramjához. A beállítás kikapcsolása esetén csak vezetékes csatlakozással lehet hozzáférni a böngészőalapú segédprogramhoz. Az eredeti **Enabled** (Bekapcsolt) beállítás meghagyásával vezeték nélküli hozzáférést biztosít a a híd böngészőalapú segédprogramjához, **Disabled** (Kikapcsolt) értékre váltásával pedig letilthatja annak vezeték nélküli elérését.

Backup and Restore (Biztonsági mentés és visszaállítás)

Backup (Biztonsági mentés) A híd konfigurációs fájljának biztonsági mentéséhez kattintson a **Backup Configurations** (Konfigurációs beállítások biztonsági mentése) gombra. Majd hajtsa végre a képernyőn megjelenő utasításokat.

Restore (Visszaállítás) Kattintson a **Browse** (Tallózás) gombra, majd válassza ki a konfigurációs fájlt. Majd kattintson a **Restore Configurations** (Konfiguráció visszaállítása) gombra.

System Reboot (Rendszer újraindítása)

Reboot (Újraindítás) A híd újraindításához kattintson a **Start to Reboot** (Indítás újraindításhoz) gombra.

A **Save Settings** (Beállítások mentése) gombbal rögzítheti a változtatásokat, míg a **Cancel Changes** (Változások elvetése) gombbal elvetheti azokat.

Administration (Felügyelet) > Factory Defaults (Gyári alapbeállítások)

Ezen a képernyőn állíthatja vissza a híd gyári alapbeállításait.

Factory Defaults (Gyári alapbeállítások)

Restore All Settings (Minden beállítás visszaállítása) A híd beállításainak alapállapotra történő visszaállításához kattintson a **Restore All Settings** (Minden beállítás visszaállítása) gombra. Minden elmentett beállítás el fog veszni, ha alaphelyzetre visszaállítja a beállításokat.



Administration (Felügyelet) > Upgrade Firmware (Eszközszoftver frissítése)

Ezen a képernyőn keresztül frissítheti a híd eszközszoftverét. Csak akkor frissítse az eszközszoftvert, ha nem működik helyesen a híd, illetve ha az új eszközszoftver valamely szolgáltatására szüksége van.



Az eszközszoftver frissítése előtt töltse le a hídhoz tartozó eszközszoftver-frissítő fájlt a Linksys weblapjáról: **www.Linksys.com/support**.

Upgrade Firmware (Eszközszoftver frissítése)

Please select a file to upgrade the firmware (Válassza ki az eszközszoftverfrissítő fájlt) Kattintson a **Browse** (Tallózás) gombra és válassza ki az eszközszoftver-frissítő fájlt. Majd kattintson a **Start to Upgrade** (Indítás rendszerfrissítéshez) gombra, majd hajtsa végre a képernyőn megjelenő utasításokat.

Status (Állapot) > Bridge (Híd)

Itt láthatók a híd adott állapotára vonatkozó adatok.



Bridge Information (Hídadatok)

Firmware Version (Eszközszoftver verziója) Itt látható a híd jelenlegi eszközszoftverének verziója.

Local Network (Helyi hálózat)

Local MAC Address (Helyi MAC-cím) Itt látható a hídnak a helyi Ethernet hálózatban megjelenő MAC-címe.

IP Address (IP-cím) Itt látható a hídnak a helyi Ethernet hálózatban megjelenő IP-címe.

Subnet Mask (Alhálózati maszk) Itt látható a helyi hálózat számára megadott alhálózati maszk.

Status (Állapot) > Wireless (Vezeték nélküli)

Itt láthatók a vezeték nélküli hálózatra vonatkozó adatok.



Wireless (Vezeték nélküli)

Link Status (Hivatkozás állapota) Itt látható a vezeték nélküli hálózathoz történő csatlakozás állapota.

MAC Address (MAC-cím) Itt látható a hídnak a helyi vezeték nélküli hálózatban megjelenő MAC-címe.

Network Name (SSID) (Hálózati név, SSID) Itt látható a vezeték nélküli hálózat neve (SSID-je).

BSSID Itt látható a csatlakoztatott vezeték nélküli útválasztónak (vagy hozzáférési pontnak) a MAC-címe.

Radio Band (Rádiósáv) Itt látható a vezeték nélküli hálózat rádiósávja.

Channel Width (Csatornaszélesség) Itt látható a vezeték nélküli hálózat által használt csatorna sávszélessége.

Wide Channel (Széles csatorna) A hálózati útválasztó csatornabeállításaitól függően itt látható a Wide Channel (Széles csatorna) jelzés. Ha az útválasztó Radio Band (Rádiósáv) vagy Channel Width (Csatornaszélesség) beállításnál a Wide – 40MHz Channel (Széles – 40 MHz-es csatorna) lehetőséget választotta, akkor ez lesz az elsődleges Wireless-N csatornája.

Standard Channel (Normál csatorna) Itt látható a normál csatorna beállítás. Ha az útválasztó Radio Band (Rádiósáv) vagy Channel Width (Csatornaszélesség) beállításnál a Wide – 40MHz Channel (Széles – 40 MHz-es csatorna) lehetőséget választotta, akkor a Standard Channel (Normál csatorna) a Wireless-N másodlagos csatornája lesz.

Bit Rate (Átviteli sebesség) Itt látható az adatátviteli sebesség.

Signal (Jel) Itt látható a jelerősség százalékban kifejezett értéke. 100% a lehető legnagyobb jelerősséget, 0% pedig a lehető legkisebb jelerősséget jelöli.

Security (Biztonság) Itt látható a vezeték nélküli hálózat biztonsági eljárása.

Hibaelhárítás

WES610N/WET610N

A számítógép vagy más vezetékes Ethernet eszköz nem képesek kommunikálni a vezeték nélküli útválasztóval.

1. Nyissa meg a híd böngészőalapú segédprogramját.
2. A *Basic Wireless Settings* (Vezeték nélküli alapbeállítások) képernyőn ellenőrizze, hogy a Network Name(Hálózatnév) (SSID) megegyezik-e a vezeték nélküli hálózat nevével.
3. Győződjön meg róla, hogy a biztonsági beállítások (WPA, WPA2 vagy WEP) megegyeznek a vezeték nélküli hálózat biztonsági beállításaival.

Meg kell változtatni a híd IP-címét.

Ha a híd DHCP-kiszolgálóval (ez rendszerint a hálózati útválasztó) kapcsolódik a hálózatra, akkor a híd a DHCP-kiszolgálótól kap IP-címet. Ha nincs DHCP-kiszolgáló, akkor a híd az alapértelmezett statikus IP-címét használja: **169.254.1.250**.

Ha azt szeretné, hogy a híd mindig statikus IP-címmel rendelkezzen, hajtsa végre az alábbi lépéseket:

1. Nyissa meg a híd böngészőalapú segédprogramját.
2. Kattintson a **Network Setup** (Hálózat beállítása) fülre.
3. Az *Network Connection Type* (Hálózati kapcsolat típusa) legördülő menüben válassza a **Static IP** (Statikus IP-cím) lehetőséget.
4. Adja meg a *Static IP Address* (Statikus IP-cím),a *Subnet Mask* (Alhálózati maszk) és a *Default Gateway* (Alapértelmezett átjáró) mezők értékét.
5. Kattintson a **Save Settings** (Beállítások mentése) gombra.

A hídhoz csatlakozó számítógép vagy más vezetékes Ethernet hálózati eszköz nem képes kommunikálni másik, vezeték nélküli eszközzel (például számítógéppel vagy nyomtatóval).

Ellenőrizze a következőket:

- Győződjön meg róla, hogy a vezeték nélküli hálózati eszköz ugyanazon a hálózaton van, mint a számítógép, vagy másik, a hídhoz csatlakozott, vezetékes Ethernet hálózati eszköz.
- Győződjön meg róla, hogy a vezeték nélküli hálózaton lévő minden eszköz ugyanazt a Network Name (SSID) hálózati nevet használja.
- Győződjön meg róla, hogy az ugyanazon az IP-hálózaton lévő minden eszköz kompatibilis IP-címet használ.

A segédprogram nem fogadja el a jelszót a weblapként megjelenő kezelőfelületen.

Ellenőrizze a következőket:

- A jelszónál különbözőnek számítanak a kis- és a nagybetűk. Ügyeljen arra, hogy megfelelő alakban adja meg a jelszó karaktereit.
- Ha elfelejti a jelszót, állítsa alaphelyzetbe a hidat.

 Mintegy öt másodpercig tartsa nyomva a híd **Reset** (Visszaállítás) gombját. Ekkor a jelszó visszaáll, értéke ismét az alapértelmezés szerinti **admin** szó lesz. A híd összes egyéb beállítása is visszaáll alaphelyzetbe. (A weblapként megjelenő kezelőfelület megnyitásához adja meg az **admin** szót a *Password* (Jelszó) mezőben.

Amikor módosításokat eszközöl a weblapként megjelenő kezelőfelületen, az új beállítások nem láthatók a képernyőn.

Kattintson a böngésző **Frissítés** gombjára. Ha nem jelennek meg az új beállítások, hajtsa végre az alábbi lépéseket:

1. Húzza ki a hálózati csatlakozót a hídból.
2. Várjon öt másodpercig, majd dugja vissza a hálózati csatlakozót a hídba.
3. Kattintson a böngésző **Frissítés** gombjára.

WEB
Ha itt nem talált választ a kérdéseire, akkor látogassa meg a Linksys weboldalát: **Linksys.com/support**

Műszaki adatok

WES610N

Modell	WES610N
Szabványok	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED-ek	Power (Tápellátás), Ethernet, Wi-Fi Protected Setup™ (Wi-Fi védelmi beállítás), Wireless (Vezeték nélkül), önálló Ethernet kapcsolat és aktivitás
Portok	Ethernet (4), hálózati csatlakozó
Gombok	Reset (Visszaállítás), Wi-Fi Protected Setup (Wi-Fi védelmi beállítás)
Kábelezés típusa	CAT5e
Antennák száma	3 (belső)
Antennacsatlakozó típusa	N/A
Lecsatlakoztatható (igen/nem)	nem
Modulációk	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF-telj. (EIRP), dBm	802.11a: 15 dBm (tipikus) @ 54Mb/s 802.11b: 19 dBm (tipikus) @ 11 Mb/s 802.11g: 16 dBm (tipikus) @ 54 Mb/s 802.11n (2.4 GHz): 18 dBm (tipikus) @ MCS15 802.11n (5 GHz): 16 dBm (tipikus) @ MCS15
Vételi érzékenység	802.11a: -72 dBm (tipikus) @ 54 Mb/s 802.11b: -85 dBm (tipikus) @ 11 Mb/s 802.11g: -73 dBm (tipikus) @ 54 Mb/s 802.11n (20 MHz): -75 dBm (tipikus) @ MCS15 802.11n (40 MHz): -69 dBm (tipikus) @ MCS15
Antenna erősítése dBi-ben	1
Vezeték nélküli biztonság	WEP, Wi-Fi Protected Access™ (Wi-Fi védett elérés) (WPA), Wi-Fi Protected Access™ 2 (Wi-Fi védett elérés 2) (WPA2)
Biztonsági kulcs hossza	Akár 128 bites titkosítás

Beépítési adatok

Méretek	177 x 128 x 68 mm (6,97" x 5,04" x 2,68")
Tömeg	295 g
Minősítés	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Tápellátás	12 V, 1 A
Üzemi hőmérséklet	0 és 40 °C között
Tárolási hőmérséklet	-20 és 60 °C között
Üzemi páratartalom	10 és 85% között (nem kicsapódó)
Tárolási páratartalom	5 és 90% között (nem kicsapódó)

A műszaki adatok bejelentés nélkül változhatnak.

WET610N

Modell	WET610N
Szabványok	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED-ek	Tápellátás, Ethernet, Wi-Fi Protected Setup™ (Wi-Fi védett telepítés), vezeték nélkül
Portok	Ethernet, hálózati csatlakozó
Gombok	Reset (Visszaállítás), Wi-Fi Protected Setup (Wi-Fi védelmi beállítás)
Kábelezés típusa	CAT5e
Antennák száma	3 (belső)
Antennacsatlakozó típusa	N/A
Lecsatlakoztatható (igen/nem)	nem
Modulációk	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF-telj. (EIRP), dBm	802.11a: 15 dBm (tipikus) @ 54Mb/s 802.11b: 18 dBm (tipikus) @ 11 Mb/s 802.11g: 16 dBm (tipikus) @ 54 Mb/s 802.11n: 12 dBm (tipikus) @ 130 Mb/s (HT20), 270 Mb/s (HT40)
Vételi érzékenység	802.11a: -72 dBm (tipikus) @ 54 Mb/s 802.11b: -85 dBm (tipikus) @ 11 Mb/s 802.11g: -73 dBm (tipikus) @ 54 Mb/s 802.11n: -70 dBm (tipikus) @ MCS15/2.4 GHz, -69 dBm (tipikus) @ MCS15/5,0 GHz
Antenna erősítése dBi-ben	1
Vezeték nélküli biztonság	WEP, Wi-Fi Protected Access™ (Wi-Fi védett elérés) (WPA), Wi-Fi Protected Access™ 2 (Wi-Fi védett elérés 2) (WPA2)
Biztonsági kulcs hossza	Akár 128 bites titkosítás

Beépítési adatok

Méretek	145 x 106 x 52 mm
Tömeg	159 g
Minősítés	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Tápellátás	12 V, 1 A
Üzemi hőmérséklet	0 és 40 °C között
Tárolási hőmérséklet	-20 és 60 °C között
Üzemi páratartalom	10 és 85% között (nem kicsapódó)
Tárolási páratartalom	5 és 90% között (nem kicsapódó)

A műszaki adatok bejelentés nélkül változhatnak.

Linksys.com/support

A Cisco, a Cisco embléma és a Linksys a Cisco és/vagy leányvállalatainak védjegye vagy bejegyzett védjegye az Egyesült Államokban és más országokban.
A Cisco védjegyeinek listája a www.cisco.com/go/trademarks webhelyen található. Minden más ebben a dokumentumban említett védjegy a megfelelő tulajdonosának tulajdona.

© 2011 Cisco és/vagy leányvállalatai. Minden jog fenntartva.

3425-01249



Panduan Pengguna

Linksys WET610N/WES610N | Jembatan Hiburan N Dua Band

Daftar Isi

Ringkasan Produk

Panel LED 2
Port LED 3

Daftar Periksa Keamanan Nirkabel

Mengubah nama jaringan nirkabel default atau SSID 4
Mengubah kata sandi default 4
Mengaktifkan pemfilteran alamat MAC 4
Mengaktifkan enkripsi 4
Panduan Keamanan Jaringan Umum 4
Tip Keamanan Tambahan 5

Konfigurasi Lanjutan

Cara mengakses utilitas berbasis browser 6
Setup (Penyetelan) > Basic Setup (Penyetelan Dasar) 7
Language (Bahasa) 7
Network Setup (Penyetelan Jaringan) 7
Wireless (Nirkabel) > Basic Wireless Settings (Setelan Nirkabel Dasar) 7
Basic Wireless Settings (Setelan Nirkabel Dasar) 8
Wireless Security (Keamanan Nirkabel) 8
Wi-Fi Protected Setup 9
Wireless (Nirkabel) > Wireless Network Site Survey (Penjajakan Lokasi Jaringan Nirkabel) 10
Wireless Network Site Survey (Penjajakan Lokasi Jaringan Nirkabel) 10
Wireless (Nirkabel) > WMM® 11
WMM 12
Wireless (Nirkabel) > Advanced Wireless Settings (Setelan Nirkabel Lanjutan) 13
Advanced Wireless (Nirkabel Lanjutan) 14
Administration (Administrasi)> Management (Manajemen) . . 14
Management (Manajemen) 14
Administration (Administrasi) > Factory Defaults (Default Pabrik) 15
Factory Defaults (Default Pabrik) 15
Administration (Administrasi) > Upgrade Firmware (Tingkatkan Firmware) 15
Upgrade Firmware (Tingkatkan Firmware) 15
Status > Bridge (Jembatan) 16
Bridge Information (Informasi Jembatan) 16
Local Network (Jaringan Lokal) 16
Status > Wireless (Nirkabel) 16
Wireless (Nirkabel) 16

Pemecahan Masalah

WES610N/WET610N 17

Spesifikasi

WES610N 18
WET610N 19

Ringkasan Produk

Terima kasih karena memilih Jembatan Hiburan N Dua Band Linksys. Jembatan dapat menghubungkan perangkat berkabel Ethernet apapun ke jaringan nirkabel Anda. Jembatan ini berbasis Wireless-N dua band, sehingga kompatibel dengan router atau titik akses Wireless-N, -G, -A, atau -B. Untuk instalasi pertama kali, ikuti langkah-langkah pada folder CD. Untuk mengkonfigurasi setelan lanjutan, gunakan utilitas berbasis browser yang praktis.

Panel LED



WES610N WET610N

Nirkabel (Biru) LED Nirkabel akan menyala bila ada koneksi nirkabel. LED akan berkedip bila jembatan secara aktif mengirim atau menerima data melalui jaringan nirkabel.

Tombol Wi-Fi Protected Setup Jika router Anda mendukung Wi-Fi Protected Setup dan menggunakan keamanan WPA atau WPA2, maka Anda dapat menggunakan Wi-Fi Protected Setup untuk menghubungkan jembatan secara otomatis. Untuk menggunakan Wi-Fi Protected Setup, lihat "Wireless (Nirkabel) > Basic Wireless Settings (Setelan Nirkabel Dasar)" pada halaman 7.

LED Wi-Fi Protected Setup (Biru/Kuning) LED akan berkedip biru selama dua menit sepanjang Wi-Fi Protected Setup. Ini akan menyala biru bila keamanan nirkabel telah diaktifkan. Jika ada kesalahan selama proses Wi-Fi Protected Setup, maka LED akan menyala kuning. Pastikan router jaringan tersebut mendukung Wi-Fi Protected Setup. Tunggu hingga LED mati, kemudian coba lagi.

Ethernet (Biru) LED Ethernet akan menyala bila ada koneksi kabel. LED akan berkedip bila jembatan secara aktif mengirim atau menerima data melalui port Ethernet.

Daya (Biru) LED Daya akan menyala bila jembatan telah dihidupkan.

Port LED



WES610N WET610N

Ethernet Port Ethernet menghubungkan jembatan ke komputer atau perangkat jaringan Ethernet lainnya. WES610N mempunyai empat port, dan WET610N mempunyai satu port.

Setel Ulang Ada dua cara untuk menyetel ulang default pabrik pada jembatan. Dengan menekan dan menahan tombol Setel Ulang selama kurang-lebih lima detik, atau memulihkan default dari Administration (Administrasi) > Factory Defaults (Default Pabrik) dalam utilitas berbasis browser pada jembatan. WES610N mempunyai sebuah tombol setel ulang di bagian bawah, dan WET610N mempunyai tombol setel ulang di panel port belakang.

Daya Port Daya menghubungkan jembatan ke adapter daya yang disertakan.

Daftar Periksa Keamanan Nirkabel

Jaringan nirkabel praktis dan mudah dipasang, sehingga rumah dengan akses Internet kecepatan tinggi cepat mengadopsinya. Karena jaringan nirkabel beroperasi dengan mengirim informasi melalui gelombang radio, maka jadi lebih rentan terhadap penyusup daripada jaringan berkabel biasa. Seperti halnya sinyal dari seluler atau telepon tanpa kabel Anda, sinyal dari jaringan nirkabel Anda juga dapat disadap. Karena secara fisik Anda tidak dapat mencegah seseorang agar tidak dapat menghubungkan ke jaringan nirkabel Anda, maka Anda perlu mengambil langkah-langkah tambahan untuk mengamankan jaringan Anda.

Mengubah nama jaringan nirkabel default atau SSID

Perangkat nirkabel mempunyai nama jaringan nirkabel default atau Service Set Identifier (SSID) yang disetel oleh pabrik. Inilah nama jaringan nirkabel Anda, dan panjangnya dapat mencapai 32 karakter. Produk nirkabel Linksys menggunakan **linksys** sebagai nama jaringan nirkabel default. Anda harus mengubah nama jaringan nirkabel ke sesuatu yang unik untuk membedakan jaringan nirkabel Anda dengan jaringan nirkabel lainnya yang ada di sekitar Anda, namun jangan gunakan informasi pribadi (seperti nomor tanda pengenal) karena informasi ini mungkin bisa dilihat siapa saja saat menjelajahi jaringan nirkabel.

Mengubah kata sandi default

Untuk produk nirkabel seperti titik akses dan router, Anda akan ditanya kata sandi saat ingin mengubah setelannya. Perangkat-perangkat ini telah disetel kata sandi defaultnya oleh pabrik. Kata sandi default Linksys adalah **admin**. Hacker tahu default ini dan mungkin mencoba menggunakannya untuk mengakses perangkat nirkabel Anda dan mengubah setelan jaringan Anda. Untuk menghalangi perubahan tanpa izin, sesuaikan kata sandi perangkat agar sulit ditebak.

Mengaktifkan pemfilteran alamat MAC

Router Linksys memberi Anda kemampuan untuk mengaktifkan pemfilteran alamat Media Access Control (MAC). Alamat MAC adalah serangkaian angka dan huruf unik yang diberikan pada setiap perangkat jaringan. Dengan mengaktifkan pemfilteran alamat MAC, akses jaringan nirkabel hanya diberikan untuk perangkat nirkabel dengan alamat MAC tertentu. Misalnya, Anda dapat menetapkan alamat MAC bagi setiap komputer di rumah Anda sehingga hanya komputer-komputer itu yang dapat mengakses jaringan nirkabel Anda.

Mengaktifkan enkripsi

Enkripsi melindungi data yang dikirim melalui jaringan nirkabel. Wi-Fi Protected Access (WPA/WPA2) dan Wired Equivalent Privacy (WEP) menawarkan tingkat keamanan yang berbeda untuk komunikasi nirkabel.

Jaringan yang dienkripsi dengan WPA/WPA2 lebih aman daripada jaringan yang dienkripsi dengan WEP, karena WPA/WPA2 menggunakan enkripsi kunci dinamis. Untuk melindungi informasi saat dikirim melalui gelombang, Anda harus mengaktifkan tingkat enkripsi tertinggi yang didukung oleh peralatan jaringan Anda.

WEP adalah standar enkripsi lama dan mungkin menjadi satu-satunya opsi yang tersedia pada beberapa perangkat lama yang tidak mendukung WPA.

Panduan Keamanan Jaringan Umum

Keamanan jaringan nirkabel tidak ada gunanya jika jaringan dasarnya tidak aman.

- Kata sandi melindungi semua komputer pada jaringan dan kata sandi individual melindungi file-file yang sensitif.
- Ubah kata sandi secara rutin.
- Instal perangkat lunak anti-virus dan perangkat lunak firewall pribadi.
- Nonaktifkan berbagi file (peer-to-peer). Beberapa aplikasi mungkin membuka berbagi file tanpa persetujuan dan/atau sepengetahuan Anda.

Tip Keamanan Tambahan

- Jauhkan router nirkabel, titik akses, atau gateways dari dinding luar dan jendela.
- Matikan router nirkabel, titik akses, atau gateway bila tidak sedang digunakan (di waktu malam, selama berlibur).
- Gunakan kalimat sandi yang kuat, setidaknya dengan panjang delapan karakter. Kombinasikan huruf dan angka untuk menghindari kata-kata standar yang dapat ditemukan dalam kamus.

Konfigurasi Lanjutan

Setelah menyetel jembatan dengan mengikuti langkah-langkah pada folder CD, jembatan akan siap digunakan. Walau demikian, jika Anda ingin mengubah setelan lanjutannya, gunakan utilitas berbasis browser. Bab ini menjelaskan setiap halaman Web pada utilitas dan berbagai fungsi pada setiap halaman. Anda dapat mengakses utilitas ini melalui browser Web pada komputer yang terhubung dengan jaringan jembatan.

Utilitas berbasis browser mempunyai beberapa tab utama: Setup (Penyetelan), Wireless (Nirkabel), Administration (Administrasi), dan Status. Tab tambahan akan tersedia setelah Anda mengklik salah satu tab utama.

Cara mengakses utilitas berbasis browser

Gunakan browser Web untuk mengakses utilitas berbasis browser.

Jika jembatan terhubung ke jaringan dengan server DHCP (biasanya router jaringan), maka jembatan akan memperoleh alamat IP-nya dari server DHCP. Jika tidak ada server DHCP, maka jembatan akan menggunakan alamat IP statis default, **169.254.1.250**. (Jika Anda menyetel alamat IP statis permanen pada jembatan melalui utilitas berbasis browser, maka masukkan alamat IP statis, sebagai gantinya.)

CATATAN

Jika Anda tidak mengetahui alamat IP jembatan, maka carilah alamat IP-nya dalam tabel klien DHCP pada router Anda. (Lihat dokumentasi untuk router Anda.)

Jika Anda tidak dapat menemukan alamat IP jembatan, Anda dapat menyetel ulang jembatan tersebut; tekan tombol **Reset** (Setel Ulang) pada jembatan selama kurang-lebih lima detik, dengan menggunakan klip kertas yang telah diluruskan. Ini akan menyetel ulang jembatan ke setelan default pabrik. Jembatan akan meminta alamat IP dari server DHCP (biasanya router jaringan). Jika tidak ada server DHCP yang ditemukan, maka jembatan akan menggunakan alamat IP statis default, **169.254.1.250**, sampai mendeteksi server DHCP dan ditetapkan dengan alamat IP dinamis.

Jika jembatan tidak dikaitkan dengan router dan menggunakan setelan default pabrik, hubungkan komputer ke jembatan dengan menggunakan koneksi Ethernet untuk mengakses utilitas berbasis Web. Anda nanti perlu mengkonfigurasi koneksi Ethernet pada komputer dengan alamat IP statis dan subnet mask.

Alamat IP adapter Ethernet Anda harus disetel ke alamat IP tertentu.

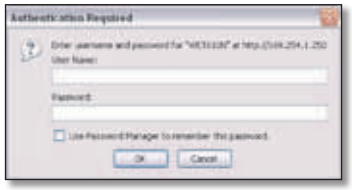
1. Dalam bidang *IP address* (Alamat IP), masukkan **169.254.x.y** (x harus diganti dengan angka, antara 1 dan 254, dan y harus diganti dengan angka, antara 0 dan 255).
2. Dalam bidang *Subnet mask* (Masker subjaringan), masukkan **255.255.0.0**.

CATATAN

Langkah-langkah untuk menetapkan alamat IP statis ke adapter Ethernet pada komputer Anda mungkin berbeda menurut sistem operasi. Untuk petunjuknya, lihat dokumentasi bantuan sistem operasi Anda.

Setelah menetapkan alamat IP statis pada adapter Ethernet, buka browser Web Anda, dan masukkan alamat IP Adapter (setelan default adalah **169.254.1.250**) dalam bidang *Address* (Alamat). Tekan **Enter**.

Layar permintaan kata sandi akan muncul. (Pengguna Non-Windows XP akan melihat layar serupa.) Biarkan bidang *User name* (Nama pengguna) kosong. Masukkan kata sandi yang telah Anda buat selama Setup Wizard (Pemandu Penyetelan). Jika Anda belum membuat kata sandi baru, gunakan kata sandi default **admin**. (Anda dapat menyetel kata sandi baru dari layar *Administration* (Administrasi) > *Management* (Manajemen).) Klik **OK** untuk melanjutkan.



CATATAN

Jika layar permintaan kata sandi tidak muncul, tunggu dua menit dan coba lagi.

Setup (Penyetelan) > Basic Setup (Penyetelan Dasar)

Layar pertama yang akan muncul adalah layar *Basic Setup* (Penyetelan Dasar). Gunakan layar ini untuk mengubah bahasa utilitas berbasis browser atau untuk mengubah setelan jaringan Ethernet yang terhubung dengan kabel ke jembatan.





Language (Bahasa)

Language (Bahasa) Ini digunakan untuk menyetel bahasa yang ditampilkan oleh utilitas berbasis browser. Pilih bahasa yang Anda inginkan dari menu turun.

Network Setup (Penyetelan Jaringan)

Bagian ini menentukan alamat IP jembatan yang diperoleh secara otomatis dari server DHCP, seperti halnya router jaringan Anda (Automatic Configuration - DHCP (Konfigurasi Otomatis - DHCP)), atau setel secara manual (Static IP (IP Statis)).

Bridge IP (IP Jembatan) Jika jaringan Anda mempunyai server DHCP, seperti halnya router jaringan Anda, menetapkan alamat IP ke perangkat jaringan Anda, maka pertahankan defaultnya, **Automatic Configuration - DHCP** (Konfigurasi Otomatis - DHCP). Jembatan akan meminta alamat IP dari server DHCP (biasanya router jaringan). Jika tidak ada server DHCP yang ditemukan, maka jembatan akan menggunakan alamat IP statis default, **169.254.1.250**, hingga ia mendeteksi server DHCP dan ditetapkan dengan alamat IP dinamis.

Jika Anda ingin menyetel alamat IP statis permanen untuk jembatan, maka pilih **Static IP** (IP Statis).

Jika Anda memilih Static IP (IP Statis), maka lengkapi bidang-bidang berikut:

- **Static IP Address** (Alamat IP Statis) Masukkan alamat IP unik yang akan digunakan untuk mengakses utilitas berbasis browser.
- **Subnet Mask** (Masker Subjaringan) Masukkan masker subjaringan dari jaringan berkabel Anda.
- **Default Gateway** (Gateway Default) (Masukkan alamat IP gateway default jaringan Anda (biasanya, ini adalah router Anda).

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Wireless (Nirkabel) > Basic Wireless Settings (Setelan Nirkabel Dasar)

Gunakan layar *Basic Wireless Settings* (Setelan Nirkabel Dasar) untuk mengkonfigurasi setelan keamanan dan setelan nirkabel dasar pada jembatan.

Ada dua cara untuk mengkonfigurasi setelan jembatan, manual dan Wi-Fi Protected Setup. Wi-Fi Protected Setup adalah fitur yang memudahkan penyetelan jaringan nirkabel Anda. Jika router jaringan Anda mendukung Wi-Fi Protected Setup dan menggunakan keamanan WPA atau WPA2, maka Anda dapat menggunakan Wi-Fi Protected Setup untuk menghubungkan jembatan secara otomatis.

Configuration View (Tampilan Konfigurasi) Untuk mengkonfigurasi jaringan nirkabel Anda secara manual, pilih **Manual**. Lihat **Basic Wireless Settings** (Setelan Nirkabel Dasar), **halaman 8**. Untuk menggunakan Wi-Fi Protected Setup, pilih **Wi-Fi Protected Setup**. Lihat **Wi-Fi Protected Setup**, **halaman 9**.

Basic Wireless Settings (Setelan Nirkabel Dasar)



Network Name (Nama Jaringan/SSID) SSID adalah nama jaringan yang dipakai bersama oleh semua titik dalam jaringan nirkabel. SSID harus sama untuk semua perangkat dalam jaringan nirkabel. SSID membedakan huruf besar dan huruf kecil dan tidak boleh melebihi 32 karakter (gunakan karakter apa saja di keyboard). Pastikan setelan ini sama dengan setelan pada router nirkabel atau titik akses. Untuk keamanan tambahan, Anda harus mengubah SSID default (**linksys**) ke nama yang unik.

Wireless Security (Keamanan Nirkabel)

Jembatan ini mendukung opsi keamanan nirkabel berikut: WPA Personal (WPA Pribadi), WPA2 Personal (WPA2 Pribadi, dan WEP. WPA (Wi-Fi Protected Access) dan WPA2 adalah metode keamanan yang lebih kuat daripada WEP (Wired Equivalent Privacy). Untuk informasi lebih lanjut tentang keamanan nirkabel, lihat "Daftar Periksa Keamanan Nirkabel", halaman 4.

Security Mode (Mode Keamanan)

Pilih metode keamanan untuk jaringan nirkabel Anda. Jika Anda tidak ingin menggunakan keamanan nirkabel, biarkan defaultnya, **Disabled** (Dinonaktifkan).

CATATAN
Ingatlah bahwa setiap perangkat di jaringan nirkabel Anda HARUS menggunakan metode keamanan dan kalimat sandi/kunci yang sama, jika tidak; perangkat nirkabel tidak akan dapat berkomunikasi satu sama lain.

WPA Personal (WPA Pribadi)

WPA adalah standar keamanan yang lebih kuat dari enkripsi WEP.



Encryption (Enkripsi) WPA mendukung metode enkripsi TKIP, dengan kunci enkripsi dinamis.

Passphrase (Kalimat Sandi) Masukkan kunci yang digunakan bersama oleh jembatan dan router nirkabel atau titik akses Anda. Harus berisi 8-63 karakter.

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

WPA2 Personal (WPA2 Pribadi)

WPA2 adalah versi WPA yang lebih modern dan lebih aman.



Encryption (Enkripsi) WPA2 mendukung dua metode enkripsi TKIP dan AES, dengan kunci enkripsi dinamis. Pilih metode enkripsi, **AES** atau **TKIP atau AES**. Pilihan default adalah **AES**.

Passphrase (Kalimat Sandi) Masukkan kunci yang digunakan bersama oleh jembatan dan router nirkabel atau titik akses. Harus berisi 8-63 karakter.

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

WEP

WEP adalah metode enkripsi dasar, yang tidak seaman WPA atau WPA2.



Encryption (Enkripsi) Pilih tingkat enkripsi WEP, **40/64 bit (10 digit heksadesimal)** atau **104/128 bit (26 digit heksadesimal)**. Defaultnya adalah **40/64 bit (10 digit heksadesimal)**.

Key 1 (Kunci 1) Masukkan kunci WEP jaringan Anda.

Tx Key (Kunci Transaksi) **Key 1** (Kunci 1) adalah kunci transmisi yang digunakan oleh jembatan.

Authentication (Autentikasi) Defaultnya adalah **Auto** (Otomatis), yang memungkinkan penggunaan autentikasi Open System (Sistem Terbuka) atau Shared Key (Kunci Bersama). Pilih **Open** (Buka) untuk menggunakan autentikasi sistem; pengirim dan penerima tidak menggunakan kunci WEP untuk autentikasi. Pilih **Shared** (Bersama) untuk menggunakan autentikasi kunci bersama; pengirim dan penerima menggunakan kunci WEP untuk autentikasi.

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Wi-Fi Protected Setup

Ada dua metode yang tersedia. Gunakan metode yang berlaku untuk router yang Anda gunakan.





Metode #1

Gunakan metode ini jika router Anda dilengkapi tombol Wi-Fi Protected Setup.

1. Klik atau tekan tombol **Wi-Fi Protected Setup** pada router.
2. Dalam dua menit, klik tombol **Wi-Fi Protected Setup** pada layar *Wi-Fi Protected Setup* jembatan.
3. Setelah jembatan dikonfigurasi, klik **Close** (Tutup).

Layar *Wi-Fi Protected Setup* menampilkan Link Status (Status Sambungan), Network Name (Nama Jaringan) (SSID), dan Security method (Metode keamanan).

Metode #2

Gunakan metode ini jika router Anda meminta nomor PIN jembatan.

1. Pada **layar** *Wi-Fi Protected Setup* router, masukkan nomor PIN pada **layar** *Wi-Fi Protected Setup* jembatan. Kemudian klik **Register** (Daftar) atau tombol yang sesuai. (Juga dicantumkan di bagian bawah jembatan.)
2. Pada **layar** *Wi-Fi Protected Setup* jembatan, klik **OK**.
3. Setelah jembatan dikonfigurasi, klik **Close** (Tutup).

Layar *Wi-Fi Protected Setup* menampilkan Link Status (Status Sambungan), Network Name (Nama Jaringan) (SSID), dan Security method (Metode keamanan).

Wireless (Nirkabel) > Wireless Network Site Survey (Penjajakan Lokasi Jaringan Nirkabel)

Klik tab **Wireless Network Site Survey** (Penjajakan Lokasi Jaringan Nirkabel) untuk memulai penjajakan lokasi. Layar *Wireless Network Site Survey* (Penjajakan Lokasi Jaringan Nirkabel) akan menampilkan daftar jaringan nirkabel yang terdeteksi oleh jembatan.



Wireless Network Site Survey (Penjajakan Lokasi Jaringan Nirkabel)

Number of Wireless Networks (Jumlah Jaringan Nirkabel) Jumlah jaringan nirkabel yang terdeteksi oleh jembatan akan ditampilkan.

Select (Pilih) Untuk menghubungkan ke jaringan nirkabel, klik **Select** (Pilih). Kemudian klik **Connect** (Hubungkan).

Wireless Network Name (Nama Jaringan Nirkabel) Nama jaringan atau SSID jaringan nirkabel akan ditampilkan.

GHz Band radio dari jaringan nirkabel akan ditampilkan.

Signal (Sinyal) Persentase kekuatan sinyal akan ditampilkan. 100% adalah kekuatan sinyal terkuat; 0% adalah yang terlemah.

Security (Keamanan) Jika jaringan mendukung Wi-Fi Protected Setup, ikon Wi-Fi Protected Setup akan ditampilkan. Metode keamanan yang digunakan oleh jaringan nirkabel akan ditampilkan.

Klik **Refresh** (Perbarui) untuk memperbarui informasi di layar.

Setelah Anda memilih sebuah jaringan, klik **Connect** (Hubungkan). Layar baru akan muncul. Ikuti petunjuk untuk metode keamanan jaringan Anda.

WPA



Network Name (SSID) (Nama Jaringan) Nama dari jaringan yang Anda pilih secara otomatis akan ditampilkan.

Security Mode (Mode Keamanan) WPA Personal (WPA Pribadi) akan ditampilkan secara otomatis.

Encryption (Enkripsi) WPA mendukung metode enkripsi TKIP, dengan kunci enkripsi dinamis.

Passphrase (Kalimat Sandi) Masukkan kunci yang digunakan bersama oleh jembatan dan router nirkabel atau titik akses. Harus berisi 8-63 karakter.

Klik **Refresh** (Perbarui) untuk memperbarui informasi di layar.

Setelah Anda memasukkan setelan keamanan, klik **Connect** (Hubungkan).

WPA2



Network Name (SSID) (Nama Jaringan) Nama dari jaringan yang Anda pilih secara otomatis akan ditampilkan.

Security Mode (Mode Keamanan) WPA2 Personal (WPA2 Pribadi) akan ditampilkan secara otomatis.

Encryption (Enkripsi) WPA2 mendukung dua metode enkripsi TKIP dan AES, dengan kunci enkripsi dinamis. Pilih metode enkripsi, **AES** atau **TKIP atau AES**.

Passphrase (Kalimat Sandi) Masukkan kunci yang digunakan bersama oleh jembatan dan router nirkabel atau titik akses. Harus berisi 8-63 karakter.

Klik **Refresh** (Perbarui) untuk memperbarui informasi di layar.

Setelah Anda memasukkan setelan keamanan, klik **Connect** (Hubungkan).

WEP



Network Name (SSID) (Nama Jaringan) Nama dari jaringan yang Anda pilih secara otomatis akan ditampilkan.

Security Mode (Mode Keamanan) WEP akan ditampilkan secara otomatis.

Encryption (Enkripsi) Pilih tingkat enkripsi WEP, **40/64 bit (10 digit heksadesimal)** atau **104/128 bit (26 digit heksadesimal)**.

Key 1 (Kunci 1) Masukkan kunci WEP jaringan Anda.

Tx Key (Kunci Transaksi) **Key 1** (Kunci 1) adalah kunci transmisi yang digunakan oleh jembatan.

Authentication (Autentikasi) Defaultnya adalah **Auto** (Otomatis), yang memungkinkan penggunaan autentikasi Open System (Sistem Terbuka) atau Shared Key (Kunci Bersama). Pilih **Open** (Buka) untuk menggunakan autentikasi sistem; pengirim dan penerima tidak menggunakan kunci WEP untuk autentikasi. Pilih **Shared** (Bersama) untuk menggunakan autentikasi kunci bersama; pengirim dan penerima menggunakan kunci WEP untuk autentikasi.

Klik **Refresh** (Perbarui) untuk memperbarui informasi di layar.

Setelah Anda memasukkan setelan keamanan, klik **Connect** (Hubungkan).

Wireless (Nirkabel) > WMM®

Konfigurasi setelan Wireless MultiMedia (WMM). WMM memprioritaskan paket sesuai dengan mode aksesnya (jenis lalu lintas): Background (Latar Belakang), Best Effort (Upaya Terbaik), Video, atau Voice (Suara). Setelan ini hanya boleh disesuaikan oleh administrator ahli karena setelan yang tidak benar dapat mengurangi kinerja nirkabel.



CATATAN
Setelan pada layar *WMM* dirancang hanya untuk pengguna yang sudah mahir.

WMM

Access Mode (Mode Akses)

Anda dapat menetapkan setelan berbeda pada empat mode akses yang tersedia. Pilih mode yang ingin Anda konfigurasi: **Background** (Latar Belakang), **Best Effort** (Upaya Terbaik), **Video**, atau **Voice** (Suara). Ikuti petunjuk untuk mode yang Anda pilih.

Background (Latar Belakang)

Use Aggregation (Gunakan Agregasi) Opsi ini menentukan apakah lapisan Media Access Control (MAC) akan menyetel sesi Add Block Acknowledgement (ADDBA), atau tidak. Defaultnya adalah **No** (Tidak). Pilih **Yes** (Ya) untuk mengaktifkan opsi ini.

Accept Aggregation (Terima Agregasi) Opsi ini menentukan apakah lapisan MAC akan menerima permintaan ADDBA; atau tidak. Defaultnya adalah **Yes** (Ya). Pilih **No** (Tidak) untuk menonaktifkan opsi ini.

Max. Number of Packets in Aggregation (Jumlah Maks. Paket dalam Agregasi) Opsi ini menentukan jumlah maksimal paket (sub-bingkai) dalam agregat. Kisarannya adalah **0** hingga **7**. Defaultnya adalah **7**.

Max. Aggregation Size (Ukuran Agregasi Maks.) Opsi ini menentukan ukuran maksimal agregat (dalam byte). Kisarannya adalah **0** hingga **16.000**. Defaultnya adalah **12.000**.

Timeout Internal (Batas Waktu Internal) Opsi ini menentukan jangka waktu menutup agregat dengan "syarat penutupan" sebelum ditutup dengan timer. Kisarannya adalah **0** hingga **100** md. Defaultnya adalah **3**.

Min. Size of Packet in Aggregation (Ukuran Min. Paket dalam Agregasi) Opsi ini menentukan ukuran minimal (dalam byte) paket yang akan diakumulasikan dalam agregat. Kisarannya adalah **0** hingga **1.500**. Defaultnya adalah **10**.

ADDBA Timeout (Batas Waktu ADDBA) Opsi ini menentukan durasi yang ditunggu untuk menghentikan penyetelan ADDBA, jika tidak ada pertukaran bingkai dalam durasi ini oleh perjanjian Block Acknowledgement (ACK). Kisarannya adalah **0** hingga **65.535** md. Defaultnya adalah **0**, yang akan menonaktifkan batas waktu.

Aggregation Window Size (Ukuran Jendela Agregasi) Opsi ini menentukan jumlah maksimal paket yang dikirim tanpa mendapatkan ACK. Kisarannya adalah **0** hingga **64**. Defaultnya adalah **64**.

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Best Effort (Upaya Terbaik)

Use Aggregation (Gunakan Agregasi) Opsi ini menentukan apakah lapisan Media Access Control (MAC) akan menyetel sesi Add Block Acknowledgement (ADDBA), atau tidak. Defaultnya adalah **Yes** (Ya). Pilih **No** (Tidak) untuk menonaktifkan opsi ini.

Accept Aggregation (Terima Agregasi) Opsi ini menentukan apakah lapisan MAC akan menerima permintaan ADDBA; atau tidak. Defaultnya adalah **Yes** (Ya). Pilih **No** (Tidak) untuk menonaktifkan opsi ini.

Max. Number of Packets in Aggregation (Jumlah Maks. Paket dalam Agregasi) Opsi ini menentukan jumlah maksimal paket (sub-bingkai) dalam agregat. Kisarannya adalah **0** hingga **10**. Defaultnya adalah **10**.

Max. Aggregation Size (Ukuran Agregasi Maks.) Opsi ini menentukan ukuran maksimal agregat (dalam byte). Kisarannya adalah **0** hingga **20.000**. Defaultnya adalah **16.000**.

Timeout Internal (Batas Waktu Internal) Opsi ini menentukan jangka waktu menutup agregat dengan "syarat penutupan" sebelum ditutup dengan timer. Kisarannya adalah **0** hingga **100** md. Defaultnya adalah **3**.

Min. Size of Packet in Aggregation (Ukuran Min. Paket dalam Agregasi) Opsi ini menentukan ukuran minimal (dalam byte) paket yang akan diakumulasikan dalam agregat. Kisarannya adalah **0** hingga **1.500**. Defaultnya adalah **10**.

ADDBA Timeout (Batas Waktu ADDBA) Opsi ini menentukan durasi yang ditunggu untuk menghentikan penyetelan ADDBA, jika tidak ada pertukaran bingkai dalam durasi ini oleh perjanjian Block Acknowledgement (ACK). Kisarannya adalah **0** hingga **65.535** md. Defaultnya adalah **0**, yang akan menonaktifkan batas waktu.

Aggregation Window Size (Ukuran Jendela Agregasi) Opsi ini menentukan jumlah maksimal paket yang dikirim tanpa mendapatkan ACK. Kisarannya adalah **0** hingga **64**. Defaultnya adalah **64**.

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Video

Use Aggregation (Gunakan Agregasi) Opsi ini menentukan apakah lapisan Media Access Control (MAC) akan menyetel sesi Add Block Acknowledgement (ADDBA), atau tidak. Defaultnya adalah **Yes** (Ya). Pilih **No** (Tidak) untuk menonaktifkan opsi ini.

Accept Aggregation (Terima Agregasi) Opsi ini menentukan apakah lapisan MAC akan menerima permintaan ADDBA; atau tidak. Defaultnya adalah **Yes** (Ya). Pilih **No** (Tidak) untuk menonaktifkan opsi ini.

Max. Number of Packets in Aggregation (Jumlah Maks. Paket dalam Agregasi) Opsi ini menentukan jumlah maksimal paket (sub-bingkai) dalam agregat. Kisarannya adalah **0** hingga **7**. Defaultnya adalah **7**.

Max. Aggregation Size (Ukuran Agregasi Maks.) Opsi ini menentukan ukuran maksimal agregat (dalam byte). Kisarannya adalah **0** hingga **16.000**. Defaultnya adalah **12.000**.

Timeout Internal (Batas Waktu Internal) Opsi ini menentukan jangka waktu menutup agregat dengan "syarat penutupan" sebelum ditutup dengan timer. Kisarannya adalah **0** hingga **100** md. Defaultnya adalah **3**.

Min. Size of Packet in Aggregation (Ukuran Min. Paket dalam Agregasi) Opsi ini menentukan ukuran minimal (dalam byte) paket yang akan diakumulasikan dalam agregat. Kisarannya adalah **0** hingga **1.500**. Defaultnya adalah **10**.

ADDBA Timeout (Batas Waktu ADDBA) Opsi ini menentukan durasi yang ditunggu untuk menghentikan penyetelan ADDBA, jika tidak ada pertukaran bingkai dalam durasi ini oleh perjanjian Block Acknowledgement (ACK). Kisarannya adalah **0** hingga **65.535** md. Defaultnya adalah **0**, yang akan menonaktifkan batas waktu.

Aggregation Window Size (Ukuran Jendela Agregasi) Opsi ini menentukan jumlah maksimal paket yang dikirim tanpa mendapatkan ACK. Kisarannya adalah **0** hingga **64**. Defaultnya adalah **64**.

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Voice (Suara)

Use Aggregation (Gunakan Agregasi) Opsi ini menentukan apakah lapisan Media Access Control (MAC) akan menyetel sesi Add Block Acknowledgement (ADDBA), atau tidak. Defaultnya adalah **Yes** (Ya). Pilih **No** (Tidak) untuk menonaktifkan opsi ini.

Accept Aggregation (Terima Agregasi) Opsi ini menentukan apakah lapisan MAC akan menerima permintaan ADDBA; atau tidak. Defaultnya adalah **Yes** (Ya). Pilih **No** (Tidak) untuk menonaktifkan opsi ini.

Max. Number of Packets in Aggregation (Jumlah Maks. Paket dalam Agregasi) Opsi ini menentukan jumlah maksimal paket (sub-bingkai) dalam agregat. Kisarannya adalah **0** hingga **2**. Defaultnya adalah **2**.

Max. Aggregation Size (Ukuran Agregasi Maks.) Opsi ini menentukan ukuran maksimal agregat (dalam byte). Kisarannya adalah **0** hingga **16.000**. Defaultnya adalah **10.000**.

Timeout Internal (Batas Waktu Internal) Opsi ini menentukan jangka waktu menutup agregat dengan "syarat penutupan" sebelum ditutup dengan timer. Kisarannya adalah **0** hingga **100** md. Defaultnya adalah **10**.

Min. Size of Packet in Aggregation (Ukuran Min. Paket dalam Agregasi) Opsi ini menentukan ukuran minimal (dalam byte) paket yang akan diakumulasikan dalam agregat. Kisarannya adalah **0** hingga **1.500**. Defaultnya adalah **10**.

ADDBA Timeout (Batas Waktu ADDBA) Opsi ini menentukan durasi yang ditunggu untuk menghentikan penyetelan ADDBA, jika tidak ada pertukaran bingkai dalam durasi ini oleh perjanjian Block Acknowledgement (ACK). Kisarannya adalah **0** hingga **65.535** md. Defaultnya adalah **0**, yang akan menonaktifkan batas waktu.

Aggregation Window Size (Ukuran Jendela Agregasi) Opsi ini menentukan jumlah maksimal paket yang dikirim tanpa mendapatkan ACK. Kisarannya adalah **0** hingga **64**. Defaultnya adalah **64**.

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Wireless (Nirkabel) > Advanced Wireless Settings (Setelan Nirkabel Lanjutan)

Konfigurasi berbagai fungsi nirkabel lanjutan pada jembatan. Setelan ini hanya boleh disesuaikan oleh administrator ahli karena setelan yang tidak benar dapat mengurangi kinerja nirkabel.



CATATAN
Setelan pada layar *Advanced Wireless Settings* (Setelan Nirkabel Lanjutan) dirancang hanya untuk pengguna yang sudah mahir.

Advanced Wireless (Nirkabel Lanjutan)

Use LDPC (Gunakan LDPC) Low-Density Parity-Check Code (LDPC) mengaktifkan atau menonaktifkan koreksi kesalahan untuk mengurangi kemungkinan hilangnya data dalam saluran yang penuh derau. Algoritma Rate Adaptation (Adaptasi Laju) secara otomatis menonaktifkan pengkodean LDPC saat bekerja pada laju PHY yang tinggi (lebih tinggi dari 162). Untuk menggunakan skema koreksi kesalahan lanjutan LDCP, pertahankan defaultnya, **Yes** (Ya). JIka tidak, pilih **No** (Tidak).

ERP Protection Type (Jenis Perlindungan ERP) Opsi ini mengkonfigurasi perlindungan paket OFDM walaupun ada workstation 802.11b dalam jaringan nirkabel. Dengan mengirim paket RTS/CTS atau paket CTS2Self dalam kecepatan 802.11b, jembatan memberi tahu jaringan nirkabel bahwa paket OFDM akan dikirim dan melindungi paket dalam jaringan nirkabel. Paket RTS/CTS dan paket CTS2Self membuat overhead, yang mungkin menghasilkan throughput lebih rendah.

Opsi RTS/CTS menyediakan jangkauan lebih baik namun throughput lebih rendah bila dibandingkan dengan CTS2Self, karena opsi RTS/CTS menyertakan pengakuan dari perangkat penerima. Untuk menggunakan opsi RTS/CTS, pertahankan defaultnya, **RTS/CTS**. Opsi None (Tidak Ada) mungkin menyebabkan benturan antara paket OFDM dan paket CCK. Untuk menggunakan opsi None (Tidak Ada), pilih **None** (Tidak Ada). Untuk menggunakan opsi CTS2Self, pilih **CTS2Self**.

11n Protection Type (Jenis Perlindungan 11n) Opsi ini mengkonfigurasi perlindungan dari perangkat non-High Throughput (HT) (selain Throughput Tinggi) dalam jaringan nirkabel. Jika router nirkabel (atau titik akses) mendeteksi pengaitan perangkat lama non-HT, ia akan mengirim sinyal ke semua perangkat HT untuk menggunakan mekanisme RTS/CTS atau CTS2Self sebelum transmisi data. Fitur ini juga mendukung semua perlindungan standar 802.11n, termasuk MIMO.

Opsi RTS/CTS menyediakan jangkauan lebih baik namun throughput lebih rendah bila dibandingkan dengan CTS2Self, karena opsi RTS/CTS menyertakan pengakuan dari perangkat penerima. Untuk menggunakan opsi RTS/CTS, pertahankan defaultnya, **RTS/CTS**. Opsi None (Tidak Ada) mungkin menyebabkan benturan antara paket HT dan paket lama. Untuk menggunakan opsi None (Tidak Ada), pilih **None** (Tidak Ada). Untuk menggunakan opsi CTS2Self, pilih **CTS2Self**.

Percentage of maximal transmit power (Persentase daya transmisi maksimal) Opsi ini menyetel persentase daya transmisi maksimal relatif terhadap pembatasan domain pengatur. Misalnya, jika pembatasan domain pengatur memungkinkan transmisi hingga 20 dB, maka menyetel persentase pada 50% akan memungkinkan daya transmisi maksimal 10 dB. Pilih persentase yang ingin Anda gunakan: **12%**, **25%**, **50%**, atau **100%**. Defaultnya adalah **100%**.

QoS Classification Type (Jenis Klasifikasi QoS) Opsi ini menyetel pemetaan 802.1D atau 802.1Q dari bidang IP DSCP/TOS ke prioritas WMM (Background (Latar Belakang), Best Effects (Efek Terbaik), Video, Voice (Suara)). Pertahankan defaultnya, **802.1D**, atau pilih **802.1Q**, yang digunakan oleh banyak aliran IPTV.

Re-establish Ethernet connection when initiating wireless connection (Buat kembali koneksi Ethernet saat memulai koneksi nirkabel) Untuk memicu pencarian DHCP dari perangkat yang berada di balik jembatan, jembatan akan menyetel ulang sambungan Ethernet antara jembatan dan perangkat setiap kali koneksi nirkabel dibuat. Untuk menonaktifkan perilaku ini, pilih **No** (Tidak). Jika tidak, pertahankan defaultnya, **Yes** (Ya).

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Administration (Administrasi)> Management (Manajemen)

Gunakan layar ini untuk mengelola fungsi tertentu pada jembatan: akses ke utilitas berbasis Web, mencadangkan file konfigurasi, dan menghidupkan ulang.



Management (Manajemen)

Bridge Access (Akses Jembatan)

Gunakan kata sandi untuk melindungi akses ke utilitas berbasis browser.

Bridge Password (Kata Sandi Jembatan) Masukkan kata sandi baru untuk jembatan.

Re-enter to confirm (Masukkan lagi untuk konfirmasi) Masukkan lagi kata sandi untuk konfirmasi.

Idle Timeout (Batas Waktu Menganggur) Waktu login akan habis setelah jangka waktu tidak aktif yang Anda tetapkan. Kisarannya adalah **60** hingga **3.600** detik. Defaultnya adalah **600**.

Akses Web (Akses Web)

Access via Wireless (Akses melalui Nirkabel) Jika Anda menggunakan jembatan dalam domain publik tempat Anda memberikan akses nirkabel kepada tamu, Anda dapat menonaktifkan akses nirkabel ke utilitas berbasis browser pada jembatan. Anda hanya akan dapat mengakses utilitas berbasis browser melalui koneksi kabel jika Anda menonaktifkan setelannya. Pertahankan defaultnya, **Enabled** (Diaktifkan), untuk mengizinkan akses ke utilitas berbasis browser pada jembatan, atau pilih **Disabled** (Nonaktifkan) untuk memblokir akses nirkabel ke utilitas.

Backup and Restore (Cadangkan dan Pulihkan)

Backup (Cadangkan) Untuk mencadangkan file konfigurasi jembatan, klik **Backup Configurations** (Cadangkan Konfigurasi). Kemudian ikuti petunjuk di layar.

Restore (Pulihkan) Klik **Browse** (Cari di) dan pilih file konfigurasi. Kemudian klik **Restore Configurations** (Pulihkan Konfigurasi).

System Reboot (Hidupkan Ulang Sistem)

Reboot (Hidupkan Ulang) Untuk menghidupkan ulang atau menjalankan ulang jembatan, klik **Start to Reboot** (Mulai Hidupkan Ulang).

Klik **Save Settings** (Simpan Setelan) untuk menerapkan perubahan yang Anda lakukan, atau klik **Cancel Changes** (Batalkan Perubahan) untuk membatalkan perubahan.

Administration (Administrasi) > Factory Defaults (Default Pabrik)

Gunakan layar ini untuk memulihkan konfigurasi jembatan ke setelan default pabriknya.

Factory Defaults (Default Pabrik)

Restore All Settings (Pulihkan Semua Setelan) Untuk menyetel ulang setelan jembatan ke default pabriknya, klik **Restore All Settings** (Pulihkan Semua Setelan). Setelan apapun yang telah Anda simpan akan hilang bila setelan default dipulihkan.



Administration (Administrasi) > Upgrade Firmware (Tingkatkan Firmware)

Gunakan layar ini untuk meningkatkan firmware jembatan. Jangan tingkatkan firmware kecuali jika Anda mengalami masalah pada jembatan atau firmware baru mempunyai fitur yang ingin Anda gunakan.



Sebelum meningkatkan firmware, unduh file peningkatan firmware jembatan dari situs Web Linksys, **www.Linksys.com/support**.

Upgrade Firmware (Tingkatkan Firmware)

Harap pilih file untuk meningkatkan firmware Klik **Browse** (Cari di) dan pilih file peningkatan firmware. Kemudian klik **Start to Upgrade** (Mulai Tingkatkan) dan ikuti petunjuk di layar.

Status > Bridge (Jembatan)

Informasi status jembatan saat ini akan ditampilkan.



Bridge Information (Informasi Jembatan)

Firmware Version (Versi Firmware) Firmware jembatan saat ini akan ditampilkan.

Local Network (Jaringan Lokal)

Local MAC Address (Alamat MAC Lokal) Alamat MAC jembatan, seperti yang terlihat pada jaringan Ethernet lokal Anda, akan ditampilkan.

IP Address (Alamat IP) Alamat IP jembatan, seperti yang terlihat pada jaringan Ethernet lokal Anda, akan ditampilkan.

Subnet Mask (Masker Subjaringan) Subnet Mask (Masker Subjaringan) yang dikonfigurasi untuk jaringan lokal Anda akan ditampilkan.

Status > Wireless (Nirkabel)

Informasi tentang jaringan nirkabel Anda akan ditampilkan.



Wireless (Nirkabel)

Link Status (Status Sambungan) Status koneksi ke jaringan nirkabel Anda akan ditampilkan.

MAC Address (Alamat MAC) Alamat MAC jembatan, seperti yang terlihat pada jaringan Ethernet lokal Anda, akan ditampilkan.

Network Name (SSID) (Nama Jaringan) Nama jaringan nirkabel atau SSID Anda akan ditampilkan.

BSSID Alamat MAC nirkabel dari router nirkabel (atau titik akses) yang terhubung akan ditampilkan.

Radio Band (Band Radio) Band radio dari jaringan nirkabel Anda akan ditampilkan.

Channel Width (Lebar Saluran) Lebar saluran, dalam MHz, yang digunakan oleh jaringan nirkabel Anda akan ditampilkan.

Wide Channel (Lebar Saluran) Tergantung pada setelan saluran router jaringan Anda, Wide Channel (Lebar Saluran) akan ditampilkan. Jika Anda memilih Wide - 40MHz Channel (Lebar - Saluran 40 MHz) untuk Radio Band (Band Radio) atau setelan Channel Width (Lebar Saluran), maka ini akan menjadi saluran Wireless-N utama Anda.

Standard Channel (Saluran Standar) Setelan Standard Channel (Saluran Standar) akan ditampilkan. Jika Anda memilih Wide - 40MHz Channel (Lebar - Saluran 40 MHz) untuk Radio Band (Band Radio) atau setelan Channel Width (Lebar Saluran), maka ini akan menjadi saluran kedua untuk Wireless-N.

Bit Rate (Laju Bit) Kecepatan transmisi data akan ditampilkan.

Signal (Sinyal) Persentase kekuatan sinyal akan ditampilkan. 100% adalah kekuatan sinyal terkuat; 0% adalah yang terlemah.

Security (Keamanan) Metode keamanan jaringan nirkabel Anda akan ditampilkan.

Pemecahan Masalah

WES610N/WET610N

Komputer Anda atau perangkat berkabel Ethernet lainnya tidak dapat berkomunikasi dengan router nirkabel.

1. Akses utilitas berbasis browser pada jembatan.
2. Pada layar *Basic Wireless Settings* (Setelan Nirkabel Dasar), pastikan Network Name (Nama Jaringan) (SSID) sama dengan nama jaringan nirkabel Anda.
3. Pastikan setelan keamanan (WPA, WPA2, atau WEP) sama dengan setelan keamanan pada jaringan nirkabel Anda.

Alamat IP jembatan perlu diubah.

Jika jembatan terhubung ke jaringan dengan server DHCP (biasanya router jaringan), maka jembatan akan memperoleh alamat IP-nya dari server DHCP. Jika tidak ada server DHCP, maka jembatan akan menggunakan alamat IP statis default, **169.254.1.250**.

Jika Anda ingin agar jembatan selalu menggunakan alamat IP statis, maka ikuti petunjuk ini:

1. Akses utilitas berbasis browser pada jembatan.
2. Klik tab **Network Setup** (Penyetelan Jaringan).
3. Dari menu turun *Network Connection Type* (Jenis Koneksi Jaringan), pilih **Static IP** (IP Statis).
4. Lengkapi bidang-bidang *Static IP Address* (Alamat IP Statis), *Subnet Mask* (Masker Subjaringan), dan *Default Gateway* (Gateway Default).
5. Klik **Save Settings** (Simpan Setelan).

Komputer berkemampuan jembatan atau perangkat berkabel Ethernet lainnya tidak akan berkomunikasi dengan perangkat berkemampuan nirkabel lain (seperti komputer atau printer).

Periksa yang berikut ini:

- Pastikan perangkat berkemampuan nirkabel berada pada jaringan nirkabel yang sama dengan komputer atau perangkat berkabel Ethernet lainnya yang terhubung ke jembatan.
- Pastikan Network Name (Nama Jaringan) (SSID) yang sama digunakan untuk semua perangkat pada jaringan nirkabel.
- Pastikan semua perangkat berada pada jaringan IP yang sama, dengan menggunakan alamat IP yang kompatibel.

Utilitas berbasis browser tidak menerima kata sandi Anda.

Periksa yang berikut ini:

- Kata sandi membedakan huruf besar-kecil. Pastikan Anda menggunakan bentuk huruf yang benar saat memasukkan kata sandi.
- Jika lupa kata sandi, Anda dapat menyetel ulang jembatan ke default pabriknya.

 Tekan dan tahan tombol **Reset** (Setel Ulang) pada jembatan selama kurang-lebih lima detik; kata sandi akan disetel ulang ke default pabriknya, **admin**. Semua setelan jembatan lainnya juga akan disetel ulang ke default pabriknya. (Untuk mengakses utilitas berbasis browser, masukkan **admin** dalam bidang *Password*.)

Setelah Anda membuat perubahan melalui utilitas berbasis browser, setelan baru tidak akan ditampilkan pada layar.

Pada browser Web Anda, klik **Refresh** (Perbarui). Jika setelan baru tidak ditampilkan, maka ikuti petunjuk ini:

1. Cabut steker adapter daya dari jembatan.
2. Tunggu lima detik, kemudian tancapkan kembali adapter daya ke jembatan.
3. Pada browser Web Anda, klik **Refresh** (Perbarui).

WEB
Jika pertanyaan Anda tidak teratasi di sini, lihat ke situs Web Linksys di **Linksys.com/support**

Spesifikasi

WES610N

Model	WES610N
Standar	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED	Daya, Ethernet, Wi-Fi Protected Setup™, Nirkabel, masing-masing sambungan dan aktivitas Ethernet
Port	Ethernet (4), Daya
Tombol	Setel Ulang, Wi-Fi Protected Setup
Jenis Kabel	CAT5e
Antena	3 (internal)
Jenis Konektor Antena	N/A
Lepas-pasang (Ya/Tidak)	Tidak
Modulasi	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) dalam dBm	802.11a: 15 dBm (tipikal) @ 54 Mbps 802.11b: 19 dBm (tipikal) @ 11 Mbps 802.11g: 16 dBm (tipikal) @ 54 Mbps 802.11n (2,4 GHz): 18 dBm (tipikal) @ MCS15 802.11n (5 GHz): 16 dBm (tipikal) @ MCS15
Sensitivitas Penerimaan	802.11a: -72 dBm (tipikal) @ 54 Mbps 802.11b: -85 dBm (tipikal) @ 11 Mbps 802.11g: -73 dBm (tipikal) @ 54 Mbps 802.11n (20 MHz): -75 dBm (tipikal) @ MCS15 802.11n (40 MHz): -69 dBm (tipikal) @ MCS15
Penguatan Antena dalam dBi	1
Keamanan Nirkabel	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit Kunci Keamanan	Hingga enkripsi 128-bit

Lingkungan

Dimensi	6,97" x 5,04" x 2,68" (177 x 128 x 68 mm)
Berat	0,65 lb (295 g)
Sertifikasi	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Daya	12 V, 1 A
Suhu Pengoperasian	32 hingga 104°F (0 hingga 40°C)
Suhu Penyimpanan	-4 hingga 104°F (-20 hingga 60°C)
Kelembapan Pengoperasian	10 hingga 85% non-kondensasi
Kelembapan Penyimpanan	5 hingga 90% non-kondensasi

Spesifikasi dapat berubah sewaktu-waktu tanpa pemberitahuan.

WET610N

Model	WET610N
Standar	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED	Daya, Ethernet, Wi-Fi Protected Setup™, Nirkabel
Port	Ethernet, Daya
Tombol	Setel Ulang, Wi-Fi Protected Setup
Jenis Kabel	CAT5e
Antena	3 (internal)
Jenis Konektor Antena	N/A
Lepas-pasang (Ya/Tidak)	Tidak
Modulasi	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) dalam dBm	802.11a: 15 dBm (tipikal) @ 54 Mbps 802.11b: 18 dBm (tipikal) @ 11 Mbps 802.11g: 16 dBm (tipikal) @ 54 Mbps 802.11n: 12 dBm (tipikal) @ 130 Mbps (HT20), 270 Mbps (HT40)
Sensitivitas Penerimaan	802.11a: -72 dBm (tipikal) @ 54 Mbps 802.11b: -85 dBm (tipikal) @ 11 Mbps 802.11g: -73 dBm (tipikal) @ 54 Mbps 802.11n: -70 dBm (tipikal) @ MCS15/2,4 GHz, -69 dBm (tipikal) @ MCS15/5,0 GHz
Penguatan Antena dalam dBi	1
Keamanan Nirkabel	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit Kunci Keamanan	Hingga enkripsi 128-bit

Lingkungan

Dimensi	5,71" x 4,17" x 2,05" (145 x 106 x 52 mm)
Berat	5,61 oz (159 g)
Sertifikasi	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Daya	12 V, 1 A
Suhu Pengoperasian	32 hingga 104°F (0 hingga 40°C)
Suhu Penyimpanan	-4 hingga 104°F (-20 hingga 60°C)
Kelembapan Pengoperasian	10 hingga 85% non-kondensasi
Kelembapan Penyimpanan	5 hingga 90% non-kondensasi

Spesifikasi dapat berubah sewaktu-waktu tanpa pemberitahuan.

Linksys.com/support

Cisco, logo Cisco, dan Linksys adalah merek dagang atau merek dagang terdaftar dari Cisco dan/atau afiliasinya di Amerika Serikat dan negara-negara lainnya.
Daftar merek dagang Cisco dapat ditemukan di www.cisco.com/go/trademarks. Semua merek dagang lainnya yang disebutkan dalam dokumen ini adalah properti dari pemiliknya masing-masing.

© 2011 Cisco dan/atau afiliasinya. Hak cipta dilindungi undang-undang.

3425-01249



Guida per l'utente

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Sommario

Panoramica del prodotto

Pannello dei LED 2
Pannello delle porte 3

Lista di controllo di protezione wireless

Modificare il nome della rete wireless predefinito o SSID 4
Modificare la password predefinita 4
Attivare il filtraggio degli indirizzi MAC 4
Attivare la cifratura 4

Istruzioni generali per la protezione di rete 4
Ulteriori suggerimenti sulla protezione 5

Configurazione avanzata

Accesso all'utilità basata sul browser 6
Setup > Basic Setup (Configurazione > Configurazione di base) . . . 7
Language (Lingua) 7
Network Setup (Configurazione rete) 7
Wireless > Basic Wireless Settings (Impostazioni wireless di base) 7
Basic Wireless Settings (Impostazioni wireless di base) 8
Wireless Security (Protezione wireless) 8
Wi-Fi Protected Setup 9
Wireless > Wireless Network Site Survey (Wireless > Ricerca sito su rete wireless) 10
Wireless Network Site Survey (Ricerca sito su rete wireless) 10
Wireless > WMM® 11
WMM 12
Wireless > Advanced Wireless Settings (Wireless > Impostazioni wireless avanzate) 13
Advanced Wireless (Impostazioni wireless avanzate) 14
Administration > Management (Amministrazione > Gestione) 14
Management (Gestione) 14
Administration > Factory Defaults (Amministrazione > Impostazioni predefinite) 15
Factory Defaults (Impostazioni predefinite) 15
Administration > Factory Defaults (Amministrazione > Aggiorna firmware) 15
Upgrade Firmware (Aggiorna firmware) 15
Status > Bridge (Stato > Bridge) 16
Bridge Information (Informazioni sul bridge) 16
Local Network (Rete locale) 16
Status > Wireless (Stato > Wireless) 16
Wireless 16

Risoluzione dei problemi

WES610N/WET610N 17

Specifiche tecniche

WES610N 18
WET610N 19

Panoramica del prodotto

Grazie per aver scelto il bridge Linksys Dual-Band N Entertainment. Il bridge può collegare qualsiasi dispositivo cablato Ethernet alla rete wireless. Il bridge si basa sulla tecnologia Wireless-N Dual-Band ed è quindi compatibile con qualsiasi router o Access Point Wireless-N, -G, -A o -B. Per la prima installazione, attenersi alla procedura descritta nella cartella del CD. Per configurare le impostazioni avanzate, utilizzare la semplice utilità basata su browser.

Pannello dei LED



WES610N WET610N

Wireless (blu) Il LED Wireless si accende per indicare una connessione wireless. Il LED lampeggia durante l'invio o la ricezione di dati da parte del bridge sulla rete wireless.

Pulsante Wi-Fi Protected Setup Se il router supporta la funzione Wi-Fi Protected Setup e utilizza la protezione WPA o WPA2, è possibile utilizzare la funzione Wi-Fi Protected Setup per collegare automaticamente il bridge. Per utilizzare la funzione Wi-Fi Protected Setup, fare riferimento a "Wireless > Basic Wireless Settings (Impostazioni wireless di base)" a pagina 7.

LED di Wi-Fi Protected Setup (blu/ambra) La luce blu del LED lampeggia per due minuti durante la procedura Wi-Fi Protected Setup. Viene emessa una luce blu quando è attiva la protezione wireless. Se si verifica un errore durante la procedura Wi-Fi Protected Setup, viene emessa una luce intermittente color ambra. Assicurarsi che il router di rete supporti la funzione Wi-Fi Protected Setup. Attendere che il LED si spenga, quindi riprovare.

Ethernet (blu) Il LED Ethernet si illumina quando è attiva una connessione cablata. Il LED lampeggia durante l'invio o la ricezione di dati da parte del bridge sulle porte Ethernet.

Alimentazione (blu) Il LED di alimentazione si illumina quando il bridge viene acceso.

Pannello delle porte



WES610N WET610N

Ethernet Le porte Ethernet consentono di collegare il bridge a un computer o a un altro dispositivo di rete Ethernet. Il bridge WES610N dispone di quattro porte, mentre il bridge WET610N dispone di un'unica porta.

Reset (Ripristino) Sono disponibili due modi per ripristinare le impostazioni predefinite del bridge. Premere il pulsante Reset (Ripristino) per circa cinque secondi oppure utilizzare la schermata Administration > Factory Defaults (Amministrazione > Impostazioni predefinite) dell'utilità basata sul Web del bridge. Il bridge WES610N dispone di un pulsante Reset (Ripristino) sulla base, mentre il bridge WET610N dispone di un pulsante Reset (Ripristino) sul pannello della porta posteriore.

Alimentazione La porta di alimentazione viene utilizzata per collegare il bridge all'adattatore di corrente in dotazione.

Lista di controllo di protezione wireless

Le reti wireless sono pratiche e facili da installare: è per questo che sono sempre più utilizzate per l'accesso a Internet ad alta velocità. Poiché la connettività di rete wireless funziona inviando informazioni tramite onde radio, può essere maggiormente vulnerabile agli attacchi di intrusi rispetto alla rete cablata tradizionale. I segnali della rete wireless possono essere intercettati, proprio come i segnali dei telefoni cellulari o cordless. Dal momento che non è possibile impedire fisicamente a un utente di connettersi alla rete wireless, è importante adottare alcune misure precauzionali per rendere sicura la propria rete.

Modificare il nome della rete wireless predefinito o SSID

I dispositivi wireless hanno un nome di rete wireless predefinito o SSID (Service Set Identifier) impostato in fabbrica. Si tratta del nome della rete wireless che può avere una lunghezza massima di 32 caratteri. I prodotti wireless Linksys utilizzano **linksys** come nome di rete wireless predefinito. È opportuno sostituire il nome di rete wireless con uno univoco per distinguere la propria rete wireless dalle altre reti esistenti; tuttavia, si consiglia di non utilizzare informazioni personali (ad esempio il codice fiscale) poiché queste potrebbero essere visibili a chiunque navighi sulla rete wireless.

Modificare la password predefinita

Per i prodotti wireless, quali punti di accesso e router, viene richiesta una password per la modifica delle impostazioni. Tali dispositivi hanno una password predefinita, impostata in fabbrica. La password predefinita Linksys è **admin**. Gli hacker sono a conoscenza di questi valori predefiniti e potrebbero tentare di usarli per accedere al dispositivo wireless e modificare le impostazioni di rete. Per impedire qualsiasi modifica non autorizzata, personalizzare la password del dispositivo in modo che sia difficile da decifrare.

Attivare il filtraggio degli indirizzi MAC

I router Linksys consentono di attivare il filtro degli indirizzi MAC (Media Access Control). L'indirizzo MAC è una serie univoca di numeri e lettere assegnati a ciascun dispositivo connesso in rete. Quando il filtraggio degli indirizzi MAC è attivato, l'accesso alla rete wireless viene consentito esclusivamente ai dispositivi wireless con specifici indirizzi MAC. Ad esempio, è possibile specificare l'indirizzo MAC di ciascun computer nella propria abitazione in modo che solo tali computer possano accedere alla rete wireless.

Attivare la cifratura

La cifratura protegge i dati trasmessi su una rete wireless. I tipi di cifratura WPA/WPA2 (Wi-Fi Protected Access) e WEP (Wired Equivalent Privacy) offrono diversi livelli di protezione per la comunicazione wireless.

Una rete che utilizza la cifratura WPA/WPA2 è più sicura rispetto a una rete con cifratura WEP, poiché WPA/WPA2 utilizza la cifratura dinamica delle chiavi. Per proteggere le informazioni man mano che passano sulle onde radio, si consiglia di attivare il massimo livello di cifratura supportato dal dispositivo di rete.

WEP è uno standard di cifratura meno recente e può essere l'unica opzione disponibile per alcuni dispositivi che non supportano WPA.

Istruzioni generali per la protezione di rete

La protezione di rete wireless non ha alcuna utilità se la rete sottostante non è sicura.

- Le password proteggono tutti i computer sulla rete e singolarmente proteggono i file riservati.
- Cambiare le password periodicamente.
- Installare software antivirus e Personal Firewall.
- Disattivare la condivisione file (peer-to-peer). Alcune applicazioni possono aprire la condivisione file senza l'autorizzazione e/o la consapevolezza dell'utente.

Ulteriori suggerimenti sulla protezione

- Mantenere i router, gli Access Point e i gateway wireless lontano da muri esterni e finestre.
- Spegnere i router, i punti di accesso e i gateway wireless quando non sono utilizzati (di notte, durante le vacanze).
- Utilizzare passphrase complesse di almeno otto caratteri. Combinare lettere e numeri per evitare di usare parole comuni che possono essere facilmente trovate in un dizionario.

Configurazione avanzata

Una volta installato mediante la procedura descritta nella cartella del CD, il bridge sarà pronto per essere utilizzato. Tuttavia, per modificare le impostazioni di rete avanzate, utilizzare l'utilità basata sul browser del router. In questo capitolo vengono descritte le pagine Web dell'utilità e le funzioni principali di ogni pagina. È possibile accedere all'utilità attraverso un browser Web connesso alla rete tramite il bridge.

Le schede principali dell'utilità basata sul browser sono: Setup (Configurazione), Wireless, Administration (Amministrazione) e Status (Stato). Ulteriori schede sono disponibili all'interno delle schede principali.

Accesso all'utilità basata sul browser

Utilizzare un browser Web per accedere all'utilità basata sul Web.

Se il bridge è collegato a una rete tramite un server DHCP (solitamente il router di rete), il bridge otterrà l'indirizzo IP dal server DHCP. Qualora non fosse disponibile alcun server DHCP, il bridge utilizzerà l'indirizzo IP statico predefinito **169.254.1.250**. Se sul bridge è stato impostato un indirizzo IP statico permanente attraverso l'utilità basata sul Web, immettere l'indirizzo IP statico.

NOTA
Se non si conosce l'indirizzo IP del bridge, consultare la tabella client DHCP del router. Consultare la documentazione del router.

Se non si riesce a individuare l'indirizzo IP del bridge, quest'ultimo può essere ripristinato. Tenere premuto il pulsante **Reset** (Ripristino) sul bridge per circa cinque secondi, utilizzando la punta di un fermaglio per la carta. In questo modo verranno ripristinate le impostazioni predefinite del bridge. Il bridge richiede un indirizzo IP del server DHCP (solitamente il router di rete). Se il server DHCP non è disponibile, il bridge utilizza l'indirizzo IP statico predefinito **169.254.1.250**, fino a quando non rileva il server DHCP e gli viene assegnato un indirizzo IP dinamico.

Se il bridge non è associato a un router e utilizza le impostazioni predefinite, collegare un computer al bridge utilizzando una connessione Ethernet per accedere all'utilità basata sul Web. La connessione Ethernet del computer deve essere configurata con un indirizzo IP statico e una maschera di sottorete.

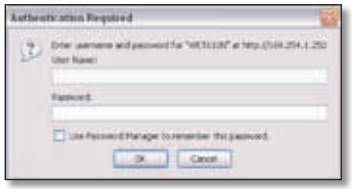
L'indirizzo IP dell'adattatore Ethernet deve essere impostato su uno specifico indirizzo IP.

1. Nel campo *IP address* (Indirizzo IP) immettere **169.254.x.y** (la variabile x sarà sostituita da un numero compreso tra 1 e 254 e y da un numero compreso tra 0 e 255).
2. Nel campo *Subnet mask* (Maschera di sottorete) immettere **255.255.0.0**.

NOTA
I passaggi per l'assegnazione di un indirizzo IP statico all'adattatore Ethernet sul computer variano in base al sistema operativo. Per istruzioni, fare riferimento alla documentazione del sistema operativo utilizzato.

Dopo avere assegnato un indirizzo IP statico all'adattatore Ethernet, lanciare il browser Web e immettere l'indirizzo IP dell'adattatore (l'indirizzo predefinito è **169.254.1.250**) nel campo *Address* (Indirizzo). Premere **Invio**.

Viene visualizzata una schermata di richiesta della password. Per gli utenti che non utilizzano Windows XP, verrà visualizzata una finestra simile. Lasciare vuoto il campo *User name* (Nome utente). Inserire la password creata durante la procedura di installazione guidata. Se non è stata creata una nuova password, utilizzare la password predefinita **admin**. È possibile impostare una nuova password nella schermata *Administration* > *Management* (Amministrazione > Gestione). Fare clic su **OK** per continuare.



NOTA
Se la schermata di richiesta della password non viene visualizzata, attendere due minuti e riprovare.

Setup > Basic Setup (Configurazione > Configurazione di base)

La prima schermata a essere visualizzata è la scheda *Basic Setup* (Configurazione di base). Utilizzare questa schermata per modificare la lingua dell'utilità basata sul Web o per modificare le impostazioni della rete Ethernet cablata del bridge.





Language (Lingua)

Language (Lingua) Questa opzione consente di impostare la lingua visualizzata dall'utilità basata su browser. Selezionare la lingua desiderata dal menu a discesa.

Network Setup (Configurazione rete)

Questa sezione determina se l'indirizzo IP del bridge viene ottenuto automaticamente da un server DHCP, ad esempio dal router di rete, Automatic Configuration - DHCP (Configurazione di rete - DHCP), o impostato manualmente, Static IP (IP statico).

Bridge IP (IP bridge) Se la rete utilizza un server DHCP, ad esempio il router di rete, per assegnare gli indirizzi IP ai dispositivi in rete, mantenere l'impostazione predefinita **Automatic Configuration - DHCP** (Configurazione automatica - DHCP). Il bridge richiede un indirizzo IP del server DHCP (solitamente il router di rete). Se il server DHCP non è disponibile, il bridge utilizza l'indirizzo IP statico predefinito **169.254.1.250**, fino a quando non rileva il server DHCP e gli viene assegnato un indirizzo IP dinamico.

Per impostare un indirizzo IP statico permanente per il bridge, selezionare **Static IP** (IP statico).

Se si seleziona questa opzione, è necessario completare i seguenti campi:

- **Static IP Address** (Indirizzo IP statico) Immettere un indirizzo IP univoco che verrà utilizzato per accedere all'utilità basata su browser.
- **Subnet Mask** (Maschera di sottorete) Inserire la maschera di sottorete della rete cablata.
- **Default Gateway** (Gateway predefinito) Immettere l'indirizzo IP del gateway predefinito per la rete (nella maggior parte dei casi è il router).

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Wireless > Basic Wireless Settings (Impostazioni wireless di base)

Utilizzare la schermata *Basic Wireless Settings* (Impostazioni wireless di base) per configurare le impostazioni wireless e di protezione di base del bridge.

Le impostazioni del bridge possono essere impostate tramite configurazione manuale e tramite Wi-Fi Protected Setup. La funzione Wi-Fi Protected Setup consente di configurare in maniera semplice la rete wireless. Se il router di rete supporta la modalità Wi-Fi Protected Setup e utilizza la protezione WPA o WPA2, è possibile utilizzare la funzione Wi-Fi Protected Setup per eseguire la connessione automatica al bridge.

Wireless Configuration (Configurazione wireless) Per configurare manualmente la rete wireless, selezionare **Manual** (Manuale). Fare riferimento a **Basic Wireless Settings** (Impostazioni wireless di base), **pagina 8**. Per utilizzare la funzione Wi-Fi Protected Setup, selezionare **Wi-Fi Protected Setup**. Fare riferimento a **Wi-Fi Protected Setup**, **pagina 9**.

Basic Wireless Settings (Impostazioni wireless di base)



Network Name - SSID (Nome di rete - SSID) Per SSID si intende il nome di rete condiviso da tutti i punti di una rete wireless e deve essere identico per tutti i dispositivi collegati in rete. Il nome è sensibile alla distinzione tra maiuscole e minuscole e non può contenere più di 32 caratteri, che possono comunque essere tutti quelli disponibili sulla tastiera. Accertarsi che questa impostazione corrisponda all'impostazione del router o del punto di accesso wireless. Per una maggiore sicurezza, si consiglia di sostituire il valore SSID predefinito (**linksys**) con un nome univoco.

Wireless Security (Protezione wireless)

Il bridge supporta le seguenti opzioni di protezione wireless: WPA Personal, WPA2 Personal e WEP. WPA (Wi-Fi Protected Access) e WPA2 sono metodi di protezione più efficaci rispetto a WEP (Wired Equivalent Privacy). Per maggiori informazioni sulla protezione wireless, fare riferimento a "Lista di controllo di protezione wireless", pagina 4.

Security Mode (Modalità di protezione)

Selezionare il metodo di protezione corretto per la rete in uso. Se non si desidera utilizzare la protezione wireless, mantenere l'impostazione predefinita **Disabled** (Disattivata).

NOTA
È importante ricordare che ogni dispositivo collegato alla rete wireless DEVE utilizzare lo stesso metodo di protezione e la stessa passphrase/chiave, altrimenti i dispositivi wireless non potranno comunicare fra loro.

WPA Personal

Il WPA è uno standard di sicurezza più efficace rispetto alla cifratura WEP.



Encryption (Cifratura) La protezione WPA supporta il metodo di cifratura TKIP, con chiavi di cifratura dinamiche.

Passphrase Immettere la chiave condivisa dal bridge e dal router wireless o Access Point. La chiave può contenere da 8 a 63 caratteri.

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

WPA2-Personal

WPA2 è la versione più sicura e avanzata di WPA.



Encryption (Cifratura) WPA2 supporta due metodi di cifratura, TKIP e AES, che utilizzano chiavi di cifratura dinamiche. Selezionare il tipo di cifratura **AES TKIP**. La selezione predefinita è **AES**.

Passphrase Immettere la chiave condivisa dal bridge e dal router wireless o Access Point. La chiave può contenere da 8 a 63 caratteri.

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

WEP

WEP è un metodo di cifratura di base meno sicuro di WPA o WPA2.



Encryption (Cifratura) Selezionare un livello di cifratura WEP, **a 40/64 bit (10 cifre esadecimali)** o **104/128 bit (26 cifre esadecimali)**. L'impostazione predefinita è **40/64 bit (10 cifre esadecimali)**.

Key 1 (Chiave 1) Immettere la chiave WEP della rete.

Tx Key (Chiave Tx) **Key 1** (Chiave 1) è la chiave di trasmissione utilizzata dal bridge.

Authentication (Autenticazione) L'impostazione predefinita è **Auto** (Automatica), che consente di utilizzare l'autenticazione Open System (Sistema aperto) o Shared Key (Chiave condivisa). Selezionare **Open** (Aperto) per utilizzare l'autenticazione con sistema aperto; il mittente e il destinatario non utilizzano una chiave WEP per l'autenticazione. Selezionare **Shared** (Condivisa) per utilizzare l'autenticazione chiave condivisa; il mittente e il destinatario utilizzano una chiave WEP per l'autenticazione.

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Wi-Fi Protected Setup

Sono disponibili due metodi. Utilizzare il metodo compatibile con il router in uso.





Metodo 1

Utilizzare questo metodo se il router è dotato di un pulsante Wi-Fi Protected Setup.

1. Fare clic o premere il pulsante **Wi-Fi Protected Setup** sul router.
2. Nell'arco di due minuti, fare clic sul pulsante **Wi-Fi Protected Setup** nella schermata *Wi-Fi Protected Setup* del bridge.
3. Una volta configurato il bridge, fare clic su **Close** (Chiudi).

La schermata *Wi-Fi Protected Setup* mostra i parametri Link Status (Stato collegamento), Network Name - SSID (Nome di rete - SSID) e Security Method (Metodo di protezione).

Metodo 2

Utilizzare questo metodo se il router richiede il numero PIN del bridge.

1. Nella schermata *Wi-Fi Protected Setup* del **router**, immettere il numero PIN nella schermata *Wi-Fi Protected Setup* del **bridge**. Quindi fare clic su **Register** (Registra) o sull'apposito pulsante (è riportato anche sull'etichetta nella parte inferiore del bridge).
2. Nella schermata *Wi-Fi Protected Setup* del **bridge**, fare clic su **OK**.
3. Una volta configurato il bridge, fare clic su **Close** (Chiudi).

La schermata *Wi-Fi Protected Setup* mostra i parametri Link Status (Stato collegamento), Network Name - SSID (Nome di rete - SSID) e Security Method (Metodo di protezione).

Wireless > Wireless Network Site Survey (Wireless > Ricerca sito su rete wireless)

Fare clic sulla scheda **Wireless Network Site Survey** (Ricerca sito su rete wireless) per avviare la ricerca di un sito. Nella schermata *Wireless Network Site Survey* (Ricerca sito su rete wireless) vengono elencate le reti wireless rilevate dal bridge.



Wireless Network Site Survey (Ricerca sito su rete wireless)

Number of Wireless Networks (Numero di reti wireless) Visualizza il numero di reti wireless rilevate dal bridge.

Select (Seleziona) Per eseguire la connessione a una rete wireless, fare clic su **Select** (Seleziona). Quindi fare clic su **Connect** (Connetti).

Wireless Network Name (Nome della rete wireless) Visualizza il nome o il SSID della rete wireless.

GHz Visualizza la banda radio della rete wireless.

Signal (Segnale) Visualizza la potenza del segnale in percentuale. 100% e 0% indicano rispettivamente la massima e la minima potenza possibile.

Security (Protezione) Se la rete supporta la modalità Wi-Fi Protected Setup, viene visualizzata l'icona Wi-Fi Protected Setup. Viene visualizzato il metodo di protezione utilizzato dalla rete wireless.

Fare clic su **Refresh** (Aggiorna) per aggiornare le informazioni visualizzate sullo schermo.

Dopo avere selezionato una rete, fare clic su **Connect** (Connetti). Viene visualizzata una nuova schermata. Seguire le istruzioni per il metodo di protezione della rete.

WPA



Network Name - SSID (Nome di rete - SSID) Visualizza automaticamente il nome della rete selezionata.

Security Mode (Modalità di protezione) Visualizza automaticamente la modalità WPA Personal.

Encryption (Cifratura) La protezione WPA supporta il metodo di cifratura TKIP, con chiavi di cifratura dinamiche.

Passphrase Immettere la chiave condivisa dal bridge e dal router wireless o Access Point. La chiave può contenere da 8 a 63 caratteri.

Fare clic su **Refresh** (Aggiorna) per aggiornare le informazioni visualizzate sullo schermo.

Una volta immesse le impostazioni di protezione, fare clic su **Connect** (Connetti).

WPA2



Network Name - SSID (Nome di rete - SSID) Visualizza automaticamente il nome della rete selezionata.

Security Mode (Modalità di protezione) Visualizza automaticamente la modalità WPA2 Personal.

Encryption (Cifratura) WPA2 supporta due metodi di cifratura, TKIP e AES, che utilizzano chiavi di cifratura dinamiche. Selezionare il tipo di cifratura **AES TKIP**.

Passphrase Immettere la chiave condivisa dal bridge e dal router wireless o Access Point. La chiave può contenere da 8 a 63 caratteri.

Fare clic su **Refresh** (Aggiorna) per aggiornare le informazioni visualizzate sullo schermo.

Una volta immesse le impostazioni di protezione, fare clic su **Connect** (Connetti).

WEP



Network Name - SSID (Nome di rete - SSID) Visualizza automaticamente il nome della rete selezionata.

Security Mode (Modalità di protezione) Visualizza automaticamente la modalità WEP.

Encryption (Cifratura) Selezionare un livello di cifratura WEP, a **40/64 bit** (10 cifre esadecimali) o **104/128 bit** (26 cifre esadecimali).

Key 1 (Chiave 1) Immettere la chiave WEP della rete.

Tx Key (Chiave Tx) **Key 1** (Chiave 1) è la chiave di trasmissione utilizzata dal bridge.

Authentication (Autenticazione) L'impostazione predefinita è **Auto** (Automatica), che consente di utilizzare l'autenticazione Open System (Sistema aperto) o Shared Key (Chiave condivisa). Selezionare **Open** (Aperto) per utilizzare l'autenticazione con sistema aperto; il mittente e il destinatario non utilizzano una chiave WEP per l'autenticazione. Selezionare **Shared** (Condivisa) per utilizzare l'autenticazione chiave condivisa; il mittente e il destinatario utilizzano una chiave WEP per l'autenticazione.

Fare clic su **Refresh** (Aggiorna) per aggiornare le informazioni visualizzate sullo schermo.

Una volta immesse le impostazioni di protezione, fare clic su **Connect** (Connetti).

Wireless > WMM®

Configurare le impostazioni Wireless MultiMedia (WMM). WMM assegna la priorità ai pacchetti in base alla rispettiva modalità di accesso (tipo di traffico): Background, Best Effort (In base al traffico), Video o Voice (Voce). Le impostazioni devono essere modificate esclusivamente da un amministratore esperto; eventuali impostazioni errate possono compromettere le prestazioni wireless.



NOTA
Le impostazioni presenti nella schermata *WMM* sono riservate solo a utenti esperti.

WMM

Access Mode (Modalità di accesso)

È possibile assegnare diverse impostazioni alle quattro modalità di accesso disponibili. Selezionare il metodo che si desidera utilizzare: **Background**, **Best Effort** (In base al traffico), **Video** o **Voice** (Voce). Seguire le istruzioni relative alla modalità selezionata.

Background

Use Aggregation (Utilizza aggregazione) Questa opzione stabilisce se il layer Media Access Control (MAC) instaura o meno una sessione ADDBA (Add Block Acknowledgement, Aggiungi blocco acknowledgement). L'impostazione predefinita è **No**. Selezionare **Yes** (Sì) per attivare questa opzione.

Accept Aggregation (Accetta aggregazione) Questa opzione stabilisce se il layer MAC accetta o meno una richiesta ADDBA. L'impostazione predefinita è **Yes** (Sì). Selezionare **No** per disattivare questa opzione.

Max. Number of Packets in Aggregation (Numero massimo di pacchetti in aggregazione) Questa opzione stabilisce il numero massimo di pacchetti (sub-frame) nell'aggregato. L'intervallo va da **0** a **7**. L'impostazione predefinita è **7**.

Max. Aggregation Size (Dimensioni massime dell'aggregazione) Questa opzione definisce le dimensioni massime dell'aggregato (in byte). L'intervallo va da **0** a **16000**. L'impostazione predefinita è **12000**.

Timeout Interval (Intervallo timeout) Questa opzione stabilisce il timeout per la chiusura dell'aggregato con una "closing condition" (condizione di chiusura) prima che venga chiuso dal timer. L'intervallo va da **0** a **100** ms. L'impostazione predefinita è **3**.

Min. Size of Packet in Aggregation (Dimensioni minime dei pacchetti in aggregazione): questa opzione stabilisce le dimensioni minime (in byte) dei pacchetti che si accumulano nell'aggregato. L'intervallo va da **0** a **1500**. L'impostazione predefinita è **10**.

ADDBA Timeout (Timeout ADDBA) Questa opzione definisce il tempo necessario per il completamento della sessione ADDBA, in assenza di scambi di frame durante questo intervallo di tempo in base all'accordo ACK (Block Acknowledgement, Blocco acknowledgement). L'intervallo va da **0** a **65535** ms. L'impostazione predefinita è **0** e consente di disattivare la funzione di timeout.

Aggregation Window Size (Dimensioni finestra di aggregazione) Questa opzione definisce il numero massimo di pacchetti trasmessi senza ricevere ACK. L'intervallo va da **0** a **64**. L'impostazione predefinita è **64**.

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Best Effort (In base al traffico)

Use Aggregation (Utilizza aggregazione) Questa opzione stabilisce se il layer Media Access Control (MAC) instaura o meno una sessione ADDBA (Add Block Acknowledgement, Aggiungi blocco acknowledgement). L'impostazione predefinita è **Yes** (Sì). Selezionare **No** per disattivare questa opzione.

Accept Aggregation (Accetta aggregazione) Questa opzione stabilisce se il layer MAC accetta o meno una richiesta ADDBA. L'impostazione predefinita è **Yes** (Sì). Selezionare **No** per disattivare questa opzione.

Max. Number of Packets in Aggregation (Numero massimo di pacchetti in aggregazione) Questa opzione stabilisce il numero massimo di pacchetti (sub-frame) nell'aggregato. L'intervallo va da **0** a **10**. L'impostazione predefinita è **10**.

Max. Aggregation Size (Dimensioni massime dell'aggregazione) Questa opzione definisce le dimensioni massime dell'aggregato (in byte). L'intervallo va da **0** a **20000**. L'impostazione predefinita è **16000**.

Timeout Interval (Intervallo timeout) Questa opzione stabilisce il timeout per la chiusura dell'aggregato con una "closing condition" (condizione di chiusura) prima che venga chiuso dal timer. L'intervallo va da **0** a **100** ms. L'impostazione predefinita è **3**.

Min. Size of Packet in Aggregation (Dimensioni minime dei pacchetti in aggregazione): questa opzione stabilisce le dimensioni minime (in byte) dei pacchetti che si accumulano nell'aggregato. L'intervallo va da **0** a **1500**. L'impostazione predefinita è **10**.

ADDBA Timeout (Timeout ADDBA) Questa opzione definisce il tempo necessario per il completamento della sessione ADDBA, in assenza di scambi di frame durante questo intervallo di tempo in base all'accordo ACK (Block Acknowledgement, Blocco acknowledgement). L'intervallo va da **0** a **65535** ms. L'impostazione predefinita è **0** e consente di disattivare la funzione di timeout.

Aggregation Window Size (Dimensioni finestra di aggregazione) Questa opzione definisce il numero massimo di pacchetti trasmessi senza ricevere ACK. L'intervallo va da **0** a **64**. L'impostazione predefinita è **64**.

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Video

Use Aggregation (Utilizza aggregazione) Questa opzione stabilisce se il layer Media Access Control (MAC) instaura o meno una sessione ADDBA (Add Block Acknowledgement, Aggiungi blocco acknowledgement). L'impostazione predefinita è **Yes** (Sì). Selezionare **No** per disattivare questa opzione.

Accept Aggregation (Accetta aggregazione) Questa opzione stabilisce se il layer MAC accetta o meno una richiesta ADDBA. L'impostazione predefinita è **Yes** (Sì). Selezionare **No** per disattivare questa opzione.

Max. Number of Packets in Aggregation (Numero massimo di pacchetti in aggregazione) Questa opzione stabilisce il numero massimo di pacchetti (sub-frame) nell'aggregato. L'intervallo va da **0** a **7**. L'impostazione predefinita è **7**.

Max. Aggregation Size (Dimensioni massime dell'aggregazione) Questa opzione definisce le dimensioni massime dell'aggregato (in byte). L'intervallo va da **0** a **16000**. L'impostazione predefinita è **12000**.

Timeout Interval (Intervallo timeout) Questa opzione stabilisce il timeout per la chiusura dell'aggregato con una "closing condition" (condizione di chiusura) prima che venga chiuso dal timer. L'intervallo va da **0** a **100** ms. L'impostazione predefinita è **3**.

Min. Size of Packet in Aggregation (Dimensioni minime dei pacchetti in aggregazione): questa opzione stabilisce le dimensioni minime (in byte) dei pacchetti che si accumulano nell'aggregato. L'intervallo va da **0** a **1500**. L'impostazione predefinita è **10**.

ADDBA Timeout (Timeout ADDBA) Questa opzione definisce il tempo necessario per il completamento della sessione ADDBA, in assenza di scambi di frame durante questo intervallo di tempo in base all'accordo ACK (Block Acknowledgement, Blocco acknowledgement). L'intervallo va da **0** a **65535** ms. L'impostazione predefinita è **0** e consente di disattivare la funzione di timeout.

Aggregation Window Size (Dimensioni finestra di aggregazione) Questa opzione definisce il numero massimo di pacchetti trasmessi senza ricevere ACK. L'intervallo va da **0** a **64**. L'impostazione predefinita è **64**.

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Voice (Voce)

Use Aggregation (Utilizza aggregazione) Questa opzione stabilisce se il layer Media Access Control (MAC) instaura o meno una sessione ADDBA (Add Block Acknowledgement, Aggiungi blocco acknowledgement). L'impostazione predefinita è **Yes** (Sì). Selezionare **No** per disattivare questa opzione.

Accept Aggregation (Accetta aggregazione) Questa opzione stabilisce se il layer MAC accetta o meno una richiesta ADDBA. L'impostazione predefinita è **Yes** (Sì). Selezionare **No** per disattivare questa opzione.

Max. Number of Packets in Aggregation (Numero massimo di pacchetti in aggregazione) Questa opzione stabilisce il numero massimo di pacchetti (sub-frame) nell'aggregato. L'intervallo va da **0** a **2**. L'impostazione predefinita è **2**.

Max. Aggregation Size (Dimensioni massime dell'aggregazione) Questa opzione definisce le dimensioni massime dell'aggregato (in byte). L'intervallo va da **0** a **16000**. L'impostazione predefinita è **10000**.

Timeout Interval (Intervallo timeout) Questa opzione stabilisce il timeout per la chiusura dell'aggregato con una "closing condition" (condizione di chiusura) prima che venga chiuso dal timer. L'intervallo va da **0** a **100** ms. L'impostazione predefinita è **10**.

Min. Size of Packet in Aggregation (Dimensioni minime dei pacchetti in aggregazione): questa opzione stabilisce le dimensioni minime (in byte) dei pacchetti che si accumulano nell'aggregato. L'intervallo va da **0** a **1500**. L'impostazione predefinita è **10**.

ADDBA Timeout (Timeout ADDBA) Questa opzione definisce il tempo necessario per il completamento della sessione ADDBA, in assenza di scambi di frame durante questo intervallo di tempo in base all'accordo ACK (Block Acknowledgement, Blocco acknowledgement). L'intervallo va da **0** a **65535** ms. L'impostazione predefinita è **0** e consente di disattivare la funzione di timeout.

Aggregation Window Size (Dimensioni finestra di aggregazione) Questa opzione definisce il numero massimo di pacchetti trasmessi senza ricevere ACK. L'intervallo va da **0** a **64**. L'impostazione predefinita è **64**.

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Wireless > Advanced Wireless Settings (Wireless > Impostazioni wireless avanzate)

Configurare le funzioni wireless avanzate del bridge. Le impostazioni devono essere modificate esclusivamente da un amministratore esperto; eventuali impostazioni errate possono compromettere le prestazioni wireless.



NOTA
Le impostazioni presenti nella schermata *Advanced Wireless Settings* (Impostazioni wireless avanzate) sono riservate solo a utenti esperti.

Advanced Wireless (Impostazioni wireless avanzate)

Use LDPC (Utilizza LDPC) Il codice LDPC (Low-Density Parity-Check) attiva o disattiva la correzione degli errori per ridurre le probabilità di perdita dei dati in canali disturbati. L'algoritmo di adattamento della velocità disattiva automaticamente il codice LDPC quando le velocità PHY sono molto elevate (superiori a 162). Per utilizzare lo schema avanzato di correzione degli errori LDCP, mantenere l'impostazione predefinita **Yes** (Sì). In caso contrario, selezionare **No**.

ERP Protection Type (Tipo di protezione ERP) Questa opzione consente di configurare la protezione dei pacchetti OFDM nonostante la presenza di stazioni 802.11b all'interno della rete wireless. Inviando pacchetti RTS/CTS o CTS2Self a velocità 802.11b, il bridge informa la rete wireless che i pacchetti OFDM stanno per essere trasferiti e sono protetti all'interno della rete wireless. I pacchetti RTS/CTS e CTS2Self creano un traffico eccessivo, che a sua volta può provocare la riduzione delle velocità di trasferimento.

L'opzione RTS/CTS offre una copertura maggiore ma velocità di trasferimento inferiori rispetto all'opzione CTS2Self, poiché include il riconoscimento dal dispositivo ricevente. Per utilizzare l'opzione RTS/CTS, mantenere l'impostazione predefinita **RTS/CTS**. L'opzione None (Nessuna) può causare conflitti tra pacchetti OFDM e CCK. Per utilizzare questa opzione, selezionare **None** (Nessuna). Per utilizzare l'opzione CTS2Self, selezionare **CTS2Self**.

11n Protection Type (Tipo di protezione 11n) Questa opzione consente di configurare la protezione da dispositivi non HT (High Throughput) all'interno della rete wireless. Nel caso in cui il router wireless (o il punto di accesso) rilevi un'associazione di un dispositivo non HT legacy, comunicherà a tutti i dispositivi HT di utilizzare i meccanismi RTS/CTS o CTS2Self prima di ogni trasmissione dati. Questa funzione supporta anche tutte le protezioni dello standard 802.11n, inclusa la tecnologia MIMO.

L'opzione RTS/CTS offre una copertura maggiore ma velocità di trasferimento inferiori rispetto all'opzione CTS2Self, poiché include il riconoscimento dal dispositivo ricevente. Per utilizzare l'opzione RTS/CTS, mantenere l'impostazione predefinita **RTS/CTS**. L'opzione None (Nessuna) può causare conflitti tra pacchetti HT e legacy. Per utilizzare questa opzione, selezionare **None** (Nessuna). Per utilizzare l'opzione CTS2Self, selezionare **CTS2Self**.

Percentage of maximal transmit power (Percentuale di potenza di trasmissione massima) Questa opzione definisce la percentuale della massima potenza di trasmissione in base ai limiti imposti dal dominio regolatore. Per esempio se il dominio regolatore consente trasmissioni con velocità fino a 20 dB, impostare la percentuale al 50% consente una potenza di trasmissione massima di 10 dB. Selezionare la percentuale che si desidera utilizzare: **12%**, **25%**, **50%** o **100%**. L'impostazione predefinita è **100%**.

QoS Classification Type (Tipo di classificazione QoS) Questa opzione imposta la mappatura 802.1D o 802.1Q del campo IP DSCP/TOS sulle priorità WMM (Background, Best Effort, Video, Voice - Background, In base al traffico, Video, Voce). Mantenere l'impostazione predefinita **802.1D** oppure selezionare **802.1Q**, utilizzata da alcuni stream IPTV.

Re-establish Ethernet connection when initiating wireless connection (Ristabilisci connessione Ethernet all'avvio della connessione wireless) Per avviare il rilevamento DHCP dal dispositivo che si trova dietro il bridge, il bridge ripristinerà il collegamento Ethernet con il dispositivo ogni volta che viene stabilita una connessione wireless. Per disattivare tale funzione, selezionare **No**. Altrimenti, mantenere l'impostazione predefinita **Yes** (Sì).

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Administration > Management (Amministrazione > Gestione)

Utilizzare questa schermata per gestire funzioni specifiche del bridge: accedere all'utilità basata sul Web, eseguire il backup del file di configurazione e il riavvio.



Management (Gestione)

Bridge Access (Accesso al bridge)

Utilizzare una password per proteggere l'accesso all'utilità basata sul Web.

Bridge Password (Password bridge) Immettere una nuova password per il bridge.

Re-enter to confirm (Conferma password) Immettere nuovamente la password per confermarla.

Idle Timeout (Timeout inattività) L'accesso viene interrotto dopo il periodo di inattività specificato. L'intervallo va da **60** a **3600** secondi. L'impostazione predefinita è **600**.

Web Access (Accesso Web)

Access via Wireless (Accesso via wireless) Se si utilizza il bridge in un dominio pubblico che consente l'accesso wireless a utenti guest, è possibile disattivare l'accesso wireless all'utilità basata sul Web del bridge. In questo modo, l'accesso all'utilità sarà possibile solo tramite la connessione cablata. Mantenere l'impostazione predefinita **Enabled** (Attivato), per consentire l'accesso wireless all'utilità basata sul Web del bridge o selezionare **Disabled** (Disattivato) per bloccare tale accesso.

Backup and Restore (Backup e ripristino)

Backup Per eseguire il backup del file di configurazione del bridge, fare clic su **Backup Configurations** (Backup configurazioni). Quindi, seguire le istruzioni visualizzate sullo schermo.

Restore (Ripristina) Fare clic su **Browse** (Sfoglia) e selezionare il file di configurazione. Quindi fare clic su **Restore Configurations** (Ripristino configurazioni).

System Reboot (Riavvio sistema)

Reboot (Riavvio) Per riavviare il bridge, fare clic su **Start to Reboot** (Inizio riavvio).

Fare clic su **Save Settings** (Salva impostazioni) per applicare le modifiche o su **Cancel Changes** (Annulla modifiche) per annullarle.

Administration > Factory Defaults (Amministrazione > Impostazioni predefinite)

Questa schermata consente di ripristinare le impostazioni di configurazione predefinite del bridge.

Factory Defaults (Impostazioni predefinite)

Restore All Settings (Ripristina tutte le impostazioni) Per ripristinare le impostazioni predefinite del bridge, fare clic su **Restore All Settings** (Ripristina tutte le impostazioni). Le impostazioni salvate vengono perse quando si ripristinano le impostazioni predefinite.



Administration > Factory Defaults (Amministrazione > Aggiorna firmware)

Utilizzare questa schermata per aggiornare il firmware del bridge. Aggiornare il firmware solo se si sono verificati problemi con il bridge o se il nuovo firmware dispone di una funzione che si desidera utilizzare.



Prima di aggiornare il firmware, scaricare il file di aggiornamento del firmware per il bridge dal sito Web di Linksys, **www.Linksys.com/support**.

Upgrade Firmware (Aggiorna firmware)

Please select a file to upgrade the firmware (Selezionare il file per l'aggiornamento del firmware) Fare clic su **Browse** (Sfoglia) e selezionare il file di aggiornamento firmware. Quindi fare clic su **Start to Upgrade** (Avvio aggiornamento) e seguire le istruzioni visualizzate sullo schermo.

Status > Bridge (Stato > Bridge)

Visualizza le informazioni sullo stato corrente del bridge.



Bridge Information (Informazioni sul bridge)

Firmware Version (Versione del firmware) Visualizza la versione firmware corrente del bridge.

Local Network (Rete locale)

Local MAC Address (Indirizzo MAC locale) Visualizza l'indirizzo MAC del bridge, così come appare sulla rete Ethernet locale.

IP Address (Indirizzo IP) Visualizza l'indirizzo IP del bridge, così come appare sulla rete Ethernet locale.

Subnet Mask (Maschera di sottorete) Visualizza la maschera di sottorete configurata per la rete locale.

Status > Wireless (Stato > Wireless)

Visualizza le informazioni sulla rete wireless.



Wireless

Link Status (Stato collegamento) Visualizza lo stato della connessione alla rete wireless.

MAC Address (Indirizzo MAC) Visualizza l'indirizzo MAC del bridge, così come appare sulla rete wireless locale.

Network Name (SSID) (Nome di rete - SSID) Visualizza il nome della rete o SSID.

BSSID Visualizza l'indirizzo MAC wireless del router wireless connesso (o punto di accesso).

Radio Band (Banda radio) Visualizza la banda radio della rete wireless.

Channel Width (Ampiezza canale) Visualizza l'ampiezza del canale, in MHz, utilizzata dalla rete wireless locale.

Wide Channel (Canale ampio) Visualizza il canale ampio, in base alle impostazioni relative al canale del router di rete. Se è stato selezionato Wide - 40MHz Channel (Canale ampio - 40 MHz) per l'impostazione Banda radio o Ampiezza canale del router, tale impostazione sarà il canale Wireless-N primario.

Standard Channel (Canale standard) Visualizza l'impostazione relativa al canale standard. Se è stato selezionato Wide - 40MHz Channel (Canale ampio - 40 MHz) per l'impostazione Banda radio o Ampiezza canale del router, il Canale standard sarà un canale secondario per la connessione Wireless-N.

Bit Rate (Velocità in bit) Visualizza la velocità di trasferimento dati.

Signal (Segnale) Visualizza la potenza del segnale in percentuale. 100% e 0% indicano rispettivamente la massima e la minima potenza possibile.

Security (Protezione) Visualizza il metodo di protezione scelto per la rete wireless.

Risoluzione dei problemi

WES610N/WET610N

Il computer o un altro dispositivo Ethernet cablato non riesce a comunicare con il router wireless.

1. Accedere all'utilità basata sul browser del router.
2. Verificare che nella schermata *Basic Wireless Settings* (Impostazioni wireless di base) il nome della rete (SSID) corrisponda al nome della rete wireless in uso.
3. Verificare che le impostazioni di protezione (WPA, WPA2 o WEP) corrispondano alle impostazioni di protezione della rete wireless in uso.

È necessario modificare l'indirizzo IP del bridge.

Se il bridge è collegato a una rete tramite un server DHCP (solitamente il router di rete), il bridge otterrà l'indirizzo IP dal server DHCP. Qualora non fosse disponibile alcun server DHCP, il bridge utilizzerà l'indirizzo IP statico predefinito **169.254.1.250**.

Se si desidera che il bridge utilizzi sempre un indirizzo IP statico, seguire le istruzioni riportate di seguito.

1. Accedere all'utilità basata sul browser del router.
2. Fare clic sulla scheda **Network Setup** (Configurazione di rete).
3. Dal menu a discesa *Network Connection Type* (Tipo connessione di rete), selezionare **Static IP** (IP statico).
4. Completare i campi *Static IP Address* (Indirizzo IP statico), *Subnet Mask* (Maschera di sottorete) e *Default Gateway* (Gateway predefinito).
5. Fare clic su **Save Settings** (Salva impostazioni).

Il computer compatibile con il bridge o un altro dispositivo Ethernet cablato non potranno comunicare con altri dispositivi wireless, quali computer o stampanti.

Eseguire i seguenti controlli:

- Verificare che il dispositivo wireless sia sulla stessa rete wireless del computer o degli altri dispositivi cablati Ethernet connessi al bridge.
- Verificare che lo stesso nome di rete (SSID) venga utilizzato per tutti i dispositivi di rete wireless;
- Verificare che tutti i dispositivi si trovino sulla stessa rete IP e che utilizzino indirizzi IP compatibili.

L'utilità basata su browser non accetta la password.

Eseguire i seguenti controlli:

- La password è sensibile alla distinzione tra maiuscole e minuscole. Verificare che la password venga immessa utilizzando correttamente maiuscole e minuscole.
- Se si dimentica la password, è possibile ripristinare le impostazioni predefinite del bridge.

 Tenere premuto il pulsante **Reset** (Ripristino) del bridge per circa 5 secondi; verranno ripristinate le impostazioni predefinite della password **admin** e tutte le altre impostazioni del bridge. Per accedere all'utilità basata su browser, inserire **admin** nel campo *Password*.

Dopo aver apportato le modifiche tramite l'utilità basata su browser, le nuove impostazioni non vengono visualizzate sullo schermo.

Sul browser Web, fare clic su **Refresh** (Aggiorna). Qualora le nuove impostazioni non venissero visualizzate, seguire le istruzioni riportate di seguito.

1. Scollegare l'adattatore di corrente dal bridge.
2. Attendere 5 secondi, quindi ricollegare l'adattatore di corrente al bridge.
3. Sul browser Web, fare clic su **Refresh** (Aggiorna).

WEB
Se le risposte alle proprie domande non sono contenute in questa appendice, visitare il sito Web di Linksys all'indirizzo **Linksys.com/support**

Specifiche tecniche

WES610N

Modello	WES610N
Standard	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED	Alimentazione, Ethernet, Wi-Fi Protected Setup™, Wireless, attività e connessione Ethernet singola
Porte	Ethernet (4), Alimentazione
Pulsanti	Reset (Ripristino), Wi-Fi Protected Setup
Tipo di cablaggio	CAT5e
Antenne	3 interne (interne)
Tipo connettore per antenna	N/D
Rimovibile (Sì/No)	No
Modulazioni	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Alimentazione RF (EIRP) in dBm	802.11a: 15 dBm (tipica) a 54 Mbps 802.11b: 19 dBm (tipica) a 11 Mbps 802.11g: 16 dBm (tipica) a 54 Mbps 802.11n (2,4 GHz): 18 dBm (tipica) a MCS15 802.11n (5 GHz): 16 dBm (tipica) a MCS15
Capacità di ricezione	802.11a: -72 dBm (tipica) a 54 Mbps 802.11b: -85 dBm (tipica) a 11 Mbps 802.11g: -73 dBm (tipica) a 54 Mbps 802.11n (20 MHz): -75 dBm (tipica) a MCS15 802.11n (40 MHz): -69 dBm (tipica) a MCS15
Guadagno dell'antenna in dBi	1
Protezione wireless	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit chiave di sicurezza	Cifratura fino a 128 bit

Specifiche ambientali

Dimensioni	6,97" x 5,04" x 2,68" (177 x 128 x 68 mm)
Peso	295 g (0,65 libbre)
Certificazione	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentazione	12 V, 1 A
Temperatura di funzionamento	Da 0 a 40 ºC (da 32 a 104 ºF)
Temperatura di conservazione	Da -20 a 60 ºC (da -4 a 140 ºF)
Umidità d'esercizio	Dal 10% all'85%, senza condensa
Umidità di conservazione	Dal 5% al 90%, senza condensa

Le specifiche sono soggette a modifiche senza preavviso.

WET610N

Modello	WET610N
Standard	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED	Alimentazione, Ethernet, Wi-Fi Protected Setup™, Wireless
Porte	Ethernet, alimentazione
Pulsanti	Reset (Ripristino), Wi-Fi Protected Setup
Tipo di cablaggio	CAT5e
Antenne	3 interne (interne)
Tipo connettore per antenna	N/D
Rimovibile (Sì/No)	No
Modulazioni	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Alimentazione RF (EIRP) in dBm	802.11a: 15 dBm (tipica) a 54 Mbps 802.11b: 18 dBm (tipica) a 11 Mbps 802.11g: 16 dBm (tipica) a 54 Mbps 802.11n: 12 dBm (tipica) a 130 Mbps (HT20), 270 Mbps (HT40)
Capacità di ricezione	802.11a: -72 dBm (tipica) a 54 Mbps 802.11b: -85 dBm (tipica) a 11 Mbps 802.11g: -73 dBm (tipica) a 54 Mbps 802.11n: -70 dBm (tipica) a MCS15/2,4 GHz, -69 dBm (tipica) a MCS15/5 GHz
Guadagno dell'antenna in dBi	1
Protezione wireless	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit chiave di sicurezza	Cifratura fino a 128 bit

Specifiche ambientali

Dimensioni	5,71" x 4,17" x 2,05" (145 x 106 x 52 mm)
Peso	159 g (5,61 once)
Certificazione	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentazione	12 V, 1 A
Temperatura di funzionamento	Da 0 a 40 ºC (da 32 a 104 ºF)
Temperatura di conservazione	Da -20 a 60 ºC (da -4 a 140 ºF)
Umidità d'esercizio	Dal 10% all'85%, senza condensa
Umidità di conservazione	Dal 5% al 90%, senza condensa

Le specifiche sono soggette a modifiche senza preavviso.

Linksys.com/support

Cisco, il logo Cisco e Linksys sono marchi o marchi registrati di Cisco e/o dei relativi affiliati negli Stati Uniti e in altri paesi.
L'elenco dei marchi di Cisco è disponibile all'indirizzo www.cisco.com/go/trademarks. Tutti gli altri marchi menzionati nel presente documento appartengono ai rispettivi proprietari.

© 2011 Cisco e/o le relative aziende affiliate. Tutti i diritti riservati.

3425-01249



Gebruikershandleiding

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Inhoud

Productoverzicht

LED's op apparaat 2
Poorten op apparaat 3

Controlelijst voor WLAN-beveiliging

Standaardnaam of SSID van het draadloze netwerk wijzigen 4
Standaardwachtwoord wijzigen 4
MAC-adresfiltering inschakelen 4
Versleuteling inschakelen 4
Algemene richtlijnen voor netwerkbeveiliging. 4
Aanvullende beveiligingstips 5

Geavanceerde configuratie

Het browsergebaseerde hulpprogramma openen 6
Setup (Instellingen) > Basic Setup (Basisinstellingen). 7
Language (Taal) 7
Network Setup (Netwerkinstellingen) 7
Wireless (WLAN) > Basic Wireless Settings (Standaardinstellingen WLAN) 7
Basic Wireless Settings (Standaardinstellingen WLAN) 8
Wireless Security (WLAN-beveiliging) 8
Wi-Fi Protected Setup 9
Wireless (WLAN) > Wireless Network Site Survey (Site-onderzoek over draadloze netwerken) 10
Site-onderzoek over draadloze netwerken 10
Wireless (WLAN) > WMM® 11
WMM 12
Wireless (WLAN) > Advanced Wireless Settings (Geavanceerde instellingen WLAN) 13
Advanced Wireless Settings (Geavanceerde instellingen WLAN) 14
Administration (Administratie) > Management (Beheer) 14
Management (Beheer) 14
Administration (Administratie) > Factory Defaults (Fabrieksinstellingen) 15
Factory Defaults (Fabrieksinstellingen) 15
Administration (Administratie) > Upgrade Firmware (Firmware upgraden) 15
Upgrade Firmware (Firmware upgraden) 15
Status > Bridge 16
Bridge-informatie 16
Local Network (Lokaal netwerk) 16
Status > Wireless (WLAN) 16
Wireless (WLAN) 16

Probleemoplossing

WES610N/WET610N 17

Specificaties

WES610N 18
WET610N 19

Productoverzicht

Bedankt dat u hebt gekozen voor de Linksys Dual-Band N Entertainment Bridge. De bridge kan elk bekabeld Ethernetapparaat verbinden met uw draadloze netwerk. De bridge is gebaseerd op dual-band Wireless-N, waardoor deze compatibel is met een willekeurige Wireless-N, -G, -A of -B router of access point. Wanneer u het apparaat voor het eerst installeert, volgt u de stappen in de map Cd. Als u geavanceerde instellingen wilt configureren, gebruikt u het handige hulpprogramma op browserbasis.

LED's op apparaat



WES610N WET610N

Draadloos (blauw) De LED Draadloos brandt als er een draadloze verbinding is. De LED knippert als de bridge actief gegevens verzendt of ontvangt via het draadloze netwerk.

De knop Wi-Fi Protected Setup Als uw router Wi-Fi Protected Setup ondersteunt en WPA- of WPA2-beveiliging gebruikt, kunt u Wi-Fi Protected Setup gebruiken om automatisch verbinding te maken met de bridge. Raadpleeg "Wireless (WLAN) > Basic Wireless Settings (Standaardinstellingen WLAN)" op pagina 7 als u Wi-Fi Protected Setup wilt gebruiken.

De LED Wi-Fi Protected Setup (Blauw/Oranje) De LED knippert twee minuten blauw tijdens Wi-Fi Protected Setup. De LED licht blauw op als WLAN-beveiliging is ingeschakeld. Als er zich een fout voordoet tijdens het Wi-Fi Protected Setup-proces, brandt de LED oranje. Controleer of de netwerkrouter Wi-Fi Protected Setup ondersteunt. Wacht totdat de LED uit gaat en probeer het vervolgens opnieuw.

Ethernet (Blauw) De LED Ethernet brandt als er een bekabelde verbinding is. De LED knippert wanneer de bridge actief gegevens verzendt of ontvangt via de Ethernetpoort(en).

Voeding (Blauw) De LED Voeding brandt wanneer de bridge wordt ingeschakeld.

Poorten op apparaat



WES610N WET610N

Ethernet De Ethernetpoort(en) verbindt/verbinden de bridge met een computer of een ander Ethernetnetwerkapparaat. De WES610N heeft vier poorten; de WET610N heeft één poort.

Reset De fabrieksinstellingen van de bridge kunnen op twee manieren worden hersteld. U kunt ongeveer vijf seconden lang op de knop Reset drukken of de standaardwaarden herstellen vanuit het scherm Administration (Administratie) > Factory Defaults (Fabrieksinstellingen) in het browsergebaseerde hulpprogramma van de bridge. De WES610N heeft een resetknop aan de onderzijde en de WET610N heeft een resetknop op de achterzijde.

Voeding Via de poort Voeding is de bridge aangesloten op de meegeleverde netstroomadapter.

Controlelijst voor WLAN-beveiliging

Vanwege het gebruiksgemak en de gemakkelijke installatieprocedure worden er steeds meer draadloze netwerken opgezet in huizen die over een snelle internetverbinding beschikken. Deze netwerken maken gebruik van radiogolven voor de verzending van informatie en zijn daarom een gemakkelijk doelwit voor indringers. De signalen van uw draadloze netwerk kunnen worden onderschept, op dezelfde manier als bij mobiele of draadloze telefoons. Het is niet mogelijk om met fysieke maatregelen te verhinderen dat anderen verbinding met uw draadloze netwerk maken, maar u kunt uw netwerk wel op andere manieren beveiligen.

Standaardnaam of SSID van het draadloze netwerk wijzigen

Voor draadloze apparatuur wordt in de fabriek een naam voor het draadloze netwerk of SSID (Service Set Identifier) ingesteld. Dit is de naam van uw draadloze netwerk en deze mag maximaal 32 tekens lang zijn. Voor draadloze apparatuur van Linksys wordt standaard **linksys** als naam van het draadloze netwerk gebruikt. U kunt uw draadloze netwerk onderscheiden van eventuele andere draadloze netwerken in de omgeving door een unieke naam voor uw draadloze netwerk op te geven. Gebruik hiervoor geen persoonlijke informatie (zoals een fiscaal nummer), want deze informatie is zichtbaar voor iedereen die naar draadloze netwerken zoekt.

Standaardwachtwoord wijzigen

Als u de instellingen van draadloze apparatuur zoals access points en routers wilt wijzigen, wordt u om een wachtwoord gevraagd. In de fabriek wordt een standaardwachtwoord ingesteld voor deze apparatuur. Het standaardwachtwoord voor Linksys is **admin**. Hackers kennen deze standaardwaarden en kunnen deze gebruiken om toegang te krijgen tot uw draadloze apparatuur en uw netwerkinstellingen te wijzigen. U kunt deze onrechtmatige wijzigingen verhinderen door het wachtwoord van uw apparaat aan te passen, zodat onbevoegden dit moeilijk kunnen raden.

MAC-adresfiltering inschakelen

U kunt MAC-adresfiltering (Media Access Control) inschakelen voor de routers van Linksys. Het MAC-adres is een unieke reeks cijfers en letters toegekend aan elk netwerkapparaat. Als MAC-adresfiltering is ingeschakeld, is het draadloze netwerk alleen toegankelijk voor draadloze apparatuur met specifieke MAC-adressen. U kunt bijvoorbeeld een specifiek MAC-adres opgeven voor elke computer in uw huis, zodat alleen die computers toegang hebben tot uw draadloze netwerk.

Versleuteling inschakelen

De gegevens die via een draadloos netwerk worden verzonden, kunnen middels versleuteling worden beveiligd. Met Wi-Fi Protected Access (WPA/WPA2) en Wired Equivalent Privacy (WEP) beschikt u over verschillende beveiligingsniveaus voor draadloze communicatie.

Versleuteling met WPA/WPA2 biedt een betere beveiliging van uw netwerk dan WEP, omdat WPA/WPA2-versleuteling gebruikmaakt van dynamische sleutels. U moet het hoogst mogelijke beveiligingsniveau gebruiken voor de versleuteling van uw netwerkapparatuur om de door u verzonden en ontvangen informatie te beveiligen.

WEP is een oudere versleutelingsmethode die soms moet worden gebruikt voor oudere apparatuur waarop WPA niet wordt ondersteund.

Algemene richtlijnen voor netwerkbeveiliging

Beveiliging van draadloze netwerken is alleen effectief als ook het onderliggende netwerk is beveiligd.

- U kunt alle computers van het netwerk beveiligen met een wachtwoord. Bovendien kunt u bestanden met gevoelige informatie ook nog afzonderlijk beveiligen met een wachtwoord.
- Wijzig de wachtwoorden regelmatig.
- Installeer antivirussoftware en persoonlijke firewallsoftware.
- Schakel het delen van bestanden (peer-to-peer) uit. In bepaalde toepassingen wordt het delen van bestanden geactiveerd zonder uw instemming en/of zonder dat u het weet.

Aanvullende beveiligingstips

- Houd draadloze routers, access points en gateways uit de buurt van buitenmuren en ramen.
- Schakel draadloze routers, access points en gateways uit wanneer u ze niet gebruikt ('s nachts, tijdens uw vakantie).
- Gebruik sterke wachtzinnen van ten minste acht tekens. Gebruik geen woorden uit het woordenboek, maar een combinatie van cijfers en letters.

Geavanceerde configuratie

Nadat u de bridge met de installatiewizard op de cd-rom hebt geïnstalleerd, is de bridge klaar voor gebruik. Als u de geavanceerde instellingen ervan echter wilt wijzigen, gebruik dan het browsergebaseerde hulpprogramma. In dit hoofdstuk komen alle webpagina's van het hulpprogramma en de belangrijkste functies op deze pagina's aan de orde. U kunt het hulpprogramma openen via een webbrowser op een computer die via een netwerk is aangesloten op de bridge.

Het browsergebaseerde hulpprogramma heeft de volgende hoofdtabbladen: Setup (Instellingen), Wireless (WLAN), Administration (Administratie), en Status. Nadat u op één van de hoofdtabbladen hebt geklikt, worden meer tabbladen weergegeven.

Het browsergebaseerde hulpprogramma openen

Gebruik een webbrowser om het browsergebaseerde hulpprogramma te openen.

Als de bridge is aangesloten op een netwerk met een DHCP-server (meestal de netwerkrouter), wijst de DHCP-server een IP-adres toe aan de bridge. Als er geen DHCP-server is, gebruikt de bridge het standaard vast IP-adres, **169.254.1.250**. (Als u via het browsergebaseerde hulpprogramma een permanent vast IP-adres op de bridge hebt ingesteld, voert u in plaats daarvan het vaste IP-adres in.)

OPMERKING
Als u niet weet wat het IP-adres van de bridge is, kunt u dit IP-adres vinden in de DHCP clients table (Clienttabel DHCP) van uw router. (Raadpleeg de documentatie van uw router.)

Als u het IP-adres van de bridge niet kunt vinden, kunt u de bridge opnieuw instellen. Druk met een rechtgebogen paperclip ongeveer vijf seconden op de knop **Reset** op de bridge. Zo herstelt u de fabrieksinstellingen van de bridge. De bridge vraagt een IP-adres van de DHCP-server (meestal de netwerkrouter). Als er geen DHCP-server wordt gevonden, gebruikt de bridge het standaard vast IP-adres, **169.254.1.250**, totdat er een DHCP-server wordt gedetecteerd die een dynamisch IP-adres toewijst aan de bridge.

Als de bridge niet aan een router wordt gekoppeld en het apparaat de fabrieksinstellingen gebruikt, sluit u via een Ethernetverbinding een computer aan op de bridge om het web-gebaseerde hulpprogramma te openen. U dient de Ethernetverbinding op de computer te configureren met een vast IP-adres en een subnetmasker.

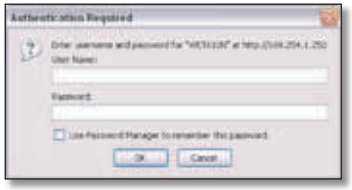
Het IP-adres van uw Ethernetadapter moet zijn ingesteld op een specifiek IP-adres.

1. Voer in het veld *IP address* (IP-adres) **169.254.x.y** in (vervang x door een getal tussen 1 en 254 en vervang y door een getal tussen 0 en 255).
2. Voer in het veld *Subnet mask* (Subnetmasker) **255.255.0.0** in.

OPMERKING
De stappen die u moet uitvoeren om een vast IP-adres toe te wijzen aan de Ethernetadapter op uw computer zijn per besturingssysteem verschillend. Raadpleeg de documentatie van uw specifieke besturingssysteem voor instructies.

Nadat u een vast IP-adres hebt toegewezen aan uw Ethernetadapter, start u uw webbrowser en geeft u het IP-adres van de adapter op (de standaardinstelling is **169.254.1.250**) in het veld *Address* (Adres). Druk op **Enter**.

Er wordt nu een scherm weergegeven waarin u uw wachtwoord kunt invoeren. (Gebruikers met een ander besturingssysteem dan Windows XP zien een soortgelijk scherm.) Laat het veld *User Name* (Gebruikersnaam) leeg. Voer het wachtwoord in dat u hebt gemaakt in de installatiewizard. Als u geen nieuw wachtwoord hebt gemaakt, gebruikt u het standaardwachtwoord **admin**. (U kunt een nieuw wachtwoord instellen vanaf het scherm *Administration* (Administratie) > *Management* (Beheer). Klik op **OK** om door te gaan.



OPMERKING
Als het scherm om uw wachtwoord in te voeren niet wordt weergegeven, wacht u twee minuten en probeert u het opnieuw.

Setup (Instellingen) > Basic Setup (Basisinstellingen)

Het eerste scherm dat wordt weergegeven, is het scherm *Basic Setup* (Basisinstellingen). Gebruik dit scherm om de taal van het browsergebaseerde hulpprogramma of de instellingen voor het bekabelde Ethernetwerk van de bridge te wijzigen.





Language (Taal)

Language (Taal) Hier kunt u de weergavetaal van het browsergebaseerde hulpprogramma wijzigen. Selecteer de gewenste taal uit het vervolgkeuzemenu.

Network Setup (Netwerkinstellingen)

Hiermee bepaalt u of een DHCP-server, bijvoorbeeld uw netwerkrouter, automatisch een IP-adres toewijst aan de bridge (Automatic Configuration - DHCP (Automatische configuratie DHCP)) of dat het IP-adres handmatig wordt ingesteld (Static IP (Vast IP-adres)).

Bridge IP (IP van bridge) Als uw netwerk een DHCP-server heeft, bijvoorbeeld uw netwerkrouter, die IP-adressen toewijst aan uw netwerkapparaten, gebruikt u de standaardinstelling **Automatic Configuration - DHCP** (Automatische configuratie DHCP). De bridge vraagt een IP-adres van de DHCP-server (meestal de netwerkrouter). Als er geen DHCP-server wordt gevonden, gebruikt de bridge het standaard vast IP-adres, **169.254.1.250**, totdat er een DHCP-server wordt gedetecteerd die een dynamisch IP-adres toewijst aan de bridge.

Selecteer **Static IP** (Vast IP-adres) als u een permanent vast IP-adres voor de bridge wilt instellen.

Als u Static IP (Vast IP-adres) selecteert, dient u de volgende velden in te vullen:

- **Static IP Address** (Vast IP-adres) Voer een uniek IP-adres in dat zal worden gebruikt om het browsergebaseerde hulpprogramma te openen.
- **Subnet Mask** (Subnetmasker) Voer het subnetmasker van uw bekabelde netwerk in.
- **Default Gateway** (Standaardgateway) Voer het IP-adres in van de standaardgateway voor uw netwerk (meestal is dit uw router).

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Wireless (WLAN) > Basic Wireless Settings (Standaardinstellingen WLAN)

Gebruik het scherm *Basic Wireless Settings* (Standaardinstellingen WLAN) om de standaard WLAN- en beveiligingsinstellingen te wijzigen.

Er zijn twee manieren om de instellingen van de bridge te configureren: handmatig en met Wi-Fi Protected Setup. Wi-Fi Protected Setup is een functie waarmee u uw draadloze netwerk op eenvoudige wijze kunt instellen. Als uw netwerkrouter Wi-Fi Protected Setup ondersteunt en WPA- of WPA2-beveiliging gebruikt, kunt u Wi-Fi Protected Setup gebruiken om automatisch verbinding te maken met de bridge.

Configuration View (Configuratieweergave) Selecteer **Manual** (Handmatig) om uw draadloze netwerk handmatig te configureren. Zie **Basic Wireless Settings** (Standaardinstellingen WLAN), **pagina 8**. Selecteer **Wi-Fi Protected Setup** als u Wi-Fi Protected Setup wilt gebruiken. Zie **Wi-Fi Protected Setup**, **pagina 9**.

Basic Wireless Settings (Standaardinstellingen WLAN)



Network Name (SSID) (Netwerknaam (SSID)) De SSID is de netwerknaam die door alle apparaten in een draadloos netwerk wordt gedeeld. Deze SSID moet voor alle apparaten in het draadloze netwerk hetzelfde zijn. De SSID is hoofdlettergevoelig en mag niet langer zijn dan 32 alfanumerieke tekens (u kunt alle tekens op het toetsenbord gebruiken). Zorg ervoor dat deze instelling overeenkomt met de instelling op uw draadloze router of access point. Voor extra veiligheid is het raadzaam de standaard-SSID (**linksys**) te wijzigen in een unieke naam.

Wireless Security (WLAN-beveiliging)

De bridge ondersteunt de volgende opties voor WLAN-beveiliging: WPA Personal, WPA2 Personal en WEP. WPA (Wi-Fi Protected Access) en WPA2 zijn sterkere beveiligingsmethoden dan WEP (Wired Equivalent Privacy). "Controlelijst voor WLAN-beveiliging", pagina 4 voor meer informatie over WLAN-beveiliging.

Beveiligingsmodus

Selecteer de juiste beveiligingsmethode voor uw draadloze netwerk. Als u geen WLAN-beveiliging wilt gebruiken, houdt u de standaardinstelling **Disabled** (Uitgeschakeld) aan.

OPMERKING
Houd er rekening mee dat elk apparaat in uw draadloze netwerk dezelfde beveiligingsmethode en wachtzin/sleutel MOET gebruiken, anders kunnen de draadloze apparaten niet met elkaar communiceren.

WPA Personal

WPA is een sterkere beveiligingsstandaard dan WEP-versleuteling.



Encryption (Versleuteling) WPA ondersteunt de TKIP-versleutelingsmethode met dynamische sleutels.

Passphrase (Wachtzin) Voer de sleutel in die door de bridge en uw draadloze router of access point wordt gedeeld. De sleutel moet uit minimaal 8 en maximaal 63 tekens bestaan.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

WPA2 Personal

WPA2 is een geavanceerdere, veiligere versie van WPA.



Encryption (Versleuteling) WPA2 ondersteunt twee versleutelingsmethoden: TKIP en AES, met dynamische versleutelingssleutels. Selecteer de versleutelingsmethode: **AES**, of **TKIP of AES**. De standaardinstelling is **AES**.

Passphrase (Wachtzin) Voer de sleutel in die door de bridge en uw draadloze router of access point wordt gedeeld. De sleutel moet uit minimaal 8 en maximaal 63 tekens bestaan.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

WEP

WEP is een basale versleutelingsmethode en minder veilig dan WPA of WPA2.



Encryption (Versleuteling) Selecteer het WEP-versleutelingsniveau dat u wilt gebruiken: **40/64 bits (10 hex digits)** (40/64-bits (10 hexadecimale tekens)) of **104/128 bits (26 hex digits)** (104/128-bits (26 hexadecimale tekens). De standaardwaarde is **40/64 bits 10 hex digits** (40/64-bits (10 hexadecimale tekens)).

Key 1 (Sleutel 1) Voer de WEP-sleutel van uw netwerk in.

Tx Key (Tx-sleutel) **Key 1** (Sleutel 1) is de zendsleutel die door de bridge wordt gebruikt.

Authentication (Verificatie) De standaardwaarde is **Auto** (Automatisch) waardoor Open System-verificatie of verificatie met een gedeelde sleutel kan worden gebruikt. Selecteer **Open** om Open System-verificatie te gebruiken. De verzender en de ontvanger gebruiken dan geen WEP-sleutel voor de verificatie. Selecteer **Shared** (Gedeeld) om verificatie met een gedeelde sleutel te gebruiken. De verzender en de ontvanger gebruiken dan wel een WEP-sleutel voor de verificatie.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Wi-Fi Protected Setup

Er zijn twee beschikbare methoden. Gebruik de juiste methode voor de router die u gebruikt.





Methode 1

Gebruik deze methode als uw router over de knop Wi-Fi Protected Setup beschikt.

1. Klik of druk op de knop **Wi-Fi Protected Setup** op de router.
2. Klik binnen twee minuten op de knop **Wi-Fi Protected Setup** in het scherm *Wi-Fi Protected Setup* op de bridge.
3. Nadat de bridge is geconfigureerd, klikt u op **Close** (Sluiten).

In het scherm *Wi-Fi Protected Setup* worden de Link Status (Verbindingsstatus), Network Name (SSID) (Netwerknaam (SSID)) en Security method (Beveiligingsmethode) weergegeven.

Methode 2

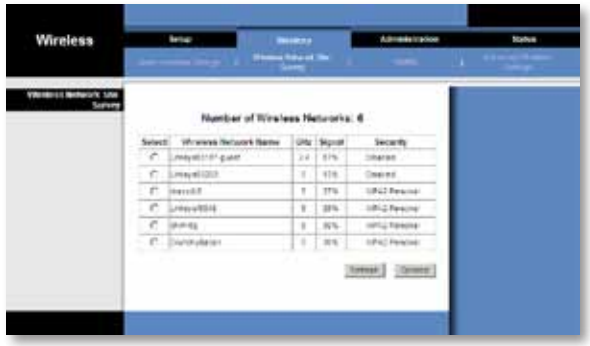
Gebruik deze methode als uw router om de PIN-code van de bridge vraagt.

1. Geef in het scherm *Wi-Fi Protected Setup* van de **router** de PIN-code op in het scherm *Wi-Fi Protected Setup* van de **bridge**. Klik vervolgens op **Register** (Aanmelden) of op de juiste knop. (Deze code staat ook op het label aan de onderkant van uw bridge.)
2. Klik in het scherm *Wi-Fi Protected Setup* van de **bridge** op **OK**.
3. Nadat de bridge is geconfigureerd, klikt u op **Close** (Sluiten).

In het scherm *Wi-Fi Protected Setup* worden de Link Status (Verbindingsstatus), Network Name (SSID) (Netwerknaam (SSID)) en Security method (Beveiligingsmethode) weergegeven.

Wireless (WLAN) > Wireless Network Site Survey (Site-onderzoek over draadloze netwerken)

Klik op het tabblad **Wireless Network Site Survey** (Site-onderzoek over draadloze netwerken) om een site-onderzoek te starten. Op het scherm *Wireless Network Site Survey* (Site-onderzoek over draadloze netwerken) vindt u een lijst met de draadloze netwerken die de bridge heeft gedetecteerd.



Site-onderzoek over draadloze netwerken

Number of Wireless Networks (Aantal draadloze netwerken) Het aantal draadloze netwerken dat de bridge heeft gedetecteerd, wordt weergegeven.

Select (Selecteren) Klik op **Select** (Selecteren) om verbinding te maken met een draadloos netwerk. Klik vervolgens op **Connect** (Verbinding maken).

Wireless Network Name (Naam WLAN) De naam van het netwerk of de SSID van het draadloze netwerk wordt weergegeven.

GHz De radioband van het draadloze netwerk wordt weergegeven.

Signal (Signaal) Het percentage van de signaalsterkte wordt weergegeven. 100% is het sterkst mogelijke signaal, 0% is het zwakst mogelijke signaal.

Security (Beveiliging) Als het netwerk Wi-Fi Protected Setup ondersteunt, wordt het pictogram Wi-Fi Protected Setup weergegeven. Hier ziet u de beveiligingsmethode die door het draadloze netwerk wordt gebruikt.

Klik op **Refresh** (Vernieuwen) als u de gegevens in het scherm wilt vernieuwen.

Klik nadat u een netwerk hebt geselecteerd op **Connect** (Verbinding maken). Er wordt een nieuw scherm weergegeven. Volg de instructies voor de beveiligingsmethode van uw netwerk.

WPA



Network Name (SSID) (Netwerknaam (SSID)) De naam van het netwerk dat u hebt geselecteerd, wordt automatisch weergegeven.

Security Mode (Beveiligingsmodus) WPA Personal wordt automatisch weergegeven.

Encryption (Versleuteling) WPA ondersteunt de TKIP-versleutelingsmethode met dynamische sleutels.

Passphrase (Wachtzin) Voer de sleutel in die door de bridge en uw draadloze router of access point wordt gedeeld. De sleutel moet uit minimaal 8 en maximaal 63 tekens bestaan.

Klik op **Refresh** (Vernieuwen) als u de gegevens in het scherm wilt vernieuwen.

Klik nadat u de beveiligingsinstellingen hebt geopend op **Connect** (Verbinding maken).

WPA2



Network Name (SSID) (Netwerknaam (SSID)) De naam van het netwerk dat u hebt geselecteerd, wordt automatisch weergegeven.

Security Mode (Beveiligingsmodus) WPA2 Personal wordt automatisch weergegeven.

Encryption (Versleuteling) WPA2 ondersteunt twee versleutelingsmethoden: TKIP en AES, met dynamische versleutelingssleutels. Selecteer de versleutelingsmethode: **AES**, of **TKIP of AES**.

Passphrase (Wachtzin) Voer de sleutel in die door de bridge en uw draadloze router of access point wordt gedeeld. De sleutel moet uit minimaal 8 en maximaal 63 tekens bestaan.

Klik op **Refresh** (Vernieuwen) als u de gegevens in het scherm wilt vernieuwen.

Klik nadat u de beveiligingsinstellingen hebt geopend op **Connect** (Verbinding maken).

WEP



Network Name (SSID) (Netwerknaam (SSID)) De naam van het netwerk dat u hebt geselecteerd, wordt automatisch weergegeven.

Security Mode (Beveiligingsmodus) WEP wordt automatisch weergegeven.

Encryption (Versleuteling) Selecteer het WEP-versleutelingsniveau dat u wilt gebruiken: **40/64 bits (10 hex digits)** (40/64-bits (10 hexadecimale tekens)) of **104/128 bits (26 hex digits)** (104/128-bits (26 hexadecimale tekens).

Key 1 (Sleutel 1) Voer de WEP-sleutel van uw netwerk in.

Tx Key (Tx-sleutel) **Key 1** (Sleutel 1) is de zendsleutel die door de bridge wordt gebruikt.

Authentication (Verificatie) De standaardwaarde is **Auto** (Automatisch) waardoor Open System-verificatie of verificatie met een gedeelde sleutel kan worden gebruikt. Selecteer **Open** om Open System-verificatie te gebruiken. De verzender en de ontvanger gebruiken dan geen WEP-sleutel voor de verificatie. Selecteer **Shared** (Gedeeld) om verificatie met een gedeelde sleutel te gebruiken. De verzender en de ontvanger gebruiken dan wel een WEP-sleutel voor de verificatie.

Klik op **Refresh** (Vernieuwen) als u de gegevens in het scherm wilt vernieuwen.

Klik nadat u de beveiligingsinstellingen hebt geopend op **Connect** (Verbinding maken).

Wireless (WLAN) > WMM®

Configureer de instellingen voor Wireless MultiMedia (WMM). WMM geeft prioriteit aan pakketten op basis van de respectieve toegangsmethoden (type verkeer): Background (Achtergrond), Best Effort (Beste poging), Video of Voice (Spraak). Deze instellingen dienen alleen door ervaren beheerders te worden aangepast, omdat bij onjuiste instellingen de prestaties van het draadloze netwerk kunnen afnemen.



OPMERKING
De instellingen in het scherm *WMM* zijn alleen geschikt voor geavanceerde gebruikers.

WMM

Access Mode (Toegangsmethode)

U kunt verschillende instellingen toewijzen aan de vier beschikbare toegangsmethoden. Selecteer de modus die u wilt configureren: **Background** (Achtergrond), **Best Effort** (Beste poging), **Video** of **Voice** (Spraak). Volg de instructies voor de geselecteerde methode.

Background (Achtergrond)

Use Aggregation (Aggregatie gebruiken) Met deze optie bepaalt u of de MAC-laag (Media Access Control) een ADDBA-sessie (Add Block Acknowledgement) configureert. De standaardinstelling is **No** (Nee). Selecteer **Yes** (Ja) om deze optie in te schakelen.

Accept Aggregation (Aggregatie accepteren) Met deze optie bepaalt u of de MAC-laag een ADDBA-verzoek accepteert. De standaardinstelling is **Yes** (Ja). Selecteer **No** (Nee) om deze optie uit te schakelen.

Max. Number of Packets in Aggregation (Maximumaantal pakketten in aggregatie) Met deze optie bepaalt u het maximumaantal pakketten (subframes) in het aggregaat. Het bereik is **0** tot **7**. De standaardinstelling is **7**.

Max. Aggregation Size (Maximale aggregatiegrootte) Met deze optie bepaalt u de maximale grootte van het aggregaat (in bytes). Het bereik is **0** tot **16.000**. De standaardinstelling is **12000**.

Timeout Interval (Time-outinterval) Met deze optie bepaalt u het time-outinterval waarmee het aggregaat dient te worden afsloten met een "afsluitvoorwaarde" voordat het wordt afgesloten door de timer. Het bereik is **0** tot **100** ms. De standaardinstelling is **3**.

Min. Size of Packet in Aggregation (Minimale pakketgrootte in aggregatie) Met deze optie bepaalt u de minimale grootte (in bytes) van de pakketten in het aggregaat. Het bereik is **0** tot **1500**. De standaardinstelling is **10**.

ADDBA Timeout (ADDBA-time-out) Met deze optie bepaalt u de tijdsperiode waarna de ADDBA-sessie wordt beëindigd als er in deze tijdsperiode geen frames worden uitgewisseld door de ACK-overeenkomst (Block Acknowledgement). Het bereik is **0** tot **65.535** ms. De standaardinstelling is **0**, waarmee u de time-out uitschakelt.

Aggregation Window Size (Grootte aggregatievenster) Met deze optie bepaalt u het maximumaantal pakketten dat wordt verzonden zonder ACK's te krijgen. Het bereik is **0** tot **64**. De standaardinstelling is **64**.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Best Effort (Beste poging)

Use Aggregation (Aggregatie gebruiken) Met deze optie bepaalt u of de MAC-laag (Media Access Control) een ADDBA-sessie (Add Block Acknowledgement) configureert. De standaardinstelling is **Yes** (Ja). Selecteer **No** (Nee) om deze optie uit te schakelen.

Accept Aggregation (Aggregatie accepteren) Met deze optie bepaalt u of de MAC-laag een ADDBA-verzoek accepteert. De standaardinstelling is **Yes** (Ja). Selecteer **No** (Nee) om deze optie uit te schakelen.

Max. Number of Packets in Aggregation (Maximumaantal pakketten in aggregatie) Met deze optie bepaalt u het maximumaantal pakketten (subframes) in het aggregaat. Het bereik is **0** tot **10**. De standaardinstelling is **10**.

Max. Aggregation Size (Maximale aggregatiegrootte) Met deze optie bepaalt u de maximale grootte van het aggregaat (in bytes). Het bereik is **0** tot **20000**. De standaardinstelling is **16000**.

Timeout Interval (Time-outinterval) Met deze optie bepaalt u het time-outinterval waarmee het aggregaat dient te worden afsloten met een "afsluitvoorwaarde" voordat het wordt afgesloten door de timer. Het bereik is **0** tot **100** ms. De standaardinstelling is **3**.

Min. Size of Packet in Aggregation (Minimale pakketgrootte in aggregatie) Met deze optie bepaalt u de minimale grootte (in bytes) van de pakketten in het aggregaat. Het bereik is **0** tot **1500**. De standaardinstelling is **10**.

ADDBA Timeout (ADDBA-time-out) Met deze optie bepaalt u de tijdsperiode waarna de ADDBA-sessie wordt beëindigd als er in deze tijdsperiode geen frames worden uitgewisseld door de ACK-overeenkomst (Block Acknowledgement). Het bereik is **0** tot **65.535** ms. De standaardinstelling is **0**, waarmee u de time-out uitschakelt.

Aggregation Window Size (Grootte aggregatievenster) Met deze optie bepaalt u het maximumaantal pakketten dat wordt verzonden zonder ACK's te krijgen. Het bereik is **0** tot **64**. De standaardinstelling is **64**.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Video

Use Aggregation (Aggregatie gebruiken) Met deze optie bepaalt u of de MAC-laag (Media Access Control) een ADDBA-sessie (Add Block Acknowledgement) configureert. De standaardinstelling is **Yes** (Ja). Selecteer **No** (Nee) om deze optie uit te schakelen.

Accept Aggregation (Aggregatie accepteren) Met deze optie bepaalt u of de MAC-laag een ADDBA-verzoek accepteert. De standaardinstelling is **Yes** (Ja). Selecteer **No** (Nee) om deze optie uit te schakelen.

Max. Number of Packets in Aggregation (Maximumaantal pakketten in aggregatie) Met deze optie bepaalt u het maximumaantal pakketten (subframes) in het aggregaat. Het bereik is **0** tot **7**. De standaardinstelling is **7**.

Max. Aggregation Size (Maximale aggregatiegrootte) Met deze optie bepaalt u de maximale grootte van het aggregaat (in bytes). Het bereik is **0** tot **16000**. De standaardinstelling is **12000**.

Timeout Interval (Time-outinterval) Met deze optie bepaalt u het time-outinterval waarmee het aggregaat dient te worden afsloten met een "afsluitvoorwaarde" voordat het wordt afgesloten door de timer. Het bereik is **0** tot **100** ms. De standaardinstelling is **3**.

Min. Size of Packet in Aggregation (Minimale pakketgrootte in aggregatie) Met deze optie bepaalt u de minimale grootte (in bytes) van de pakketten in het aggregaat. Het bereik is **0** tot **1500**. De standaardinstelling is **10**.

ADDBA Timeout (ADDBA-time-out) Met deze optie bepaalt u de tijdsperiode waarna de ADDBA-sessie wordt beëindigd als er in deze tijdsperiode geen frames worden uitgewisseld door de ACK-overeenkomst (Block Acknowledgement). Het bereik is **0** tot **65.535** ms. De standaardinstelling is **0**, waarmee u de time-out uitschakelt.

Aggregation Window Size (Grootte aggregatievenster) Met deze optie bepaalt u het maximumaantal pakketten dat wordt verzonden zonder ACK's te krijgen. Het bereik is **0** tot **64**. De standaardinstelling is **64**.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Voice (Spraak)

Use Aggregation (Aggregatie gebruiken) Met deze optie bepaalt u of de MAC-laag (Media Access Control) een ADDBA-sessie (Add Block Acknowledgement) configureert. De standaardinstelling is **Yes** (Ja). Selecteer **No** (Nee) om deze optie uit te schakelen.

Accept Aggregation (Aggregatie accepteren) Met deze optie bepaalt u of de MAC-laag een ADDBA-verzoek accepteert. De standaardinstelling is **Yes** (Ja). Selecteer **No** (Nee) om deze optie uit te schakelen.

Max. Number of Packets in Aggregation (Maximumaantal pakketten in aggregatie) Met deze optie bepaalt u het maximumaantal pakketten (subframes) in het aggregaat. Het bereik is **0** tot **2**. De standaardinstelling is **2**.

Max. Aggregation Size (Maximale aggregatiegrootte) Met deze optie bepaalt u de maximale grootte van het aggregaat (in bytes). Het bereik is **0** tot **16000**. De standaardinstelling is **10000**.

Timeout Interval (Time-outinterval) Met deze optie bepaalt u het time-outinterval waarmee het aggregaat dient te worden afsloten met een "afsluitvoorwaarde" voordat het wordt afgesloten door de timer. Het bereik is **0** tot **100** ms. De standaardinstelling is **10**.

Min. Size of Packet in Aggregation (Minimale pakketgrootte in aggregatie) Met deze optie bepaalt u de minimale grootte (in bytes) van de pakketten in het aggregaat. Het bereik is **0** tot **1500**. De standaardinstelling is **10**.

ADDBA Timeout (ADDBA-time-out) Met deze optie bepaalt u de tijdsperiode waarna de ADDBA-sessie wordt beëindigd als er in deze tijdsperiode geen frames worden uitgewisseld door de ACK-overeenkomst (Block Acknowledgement). Het bereik is **0** tot **65.535** ms. De standaardinstelling is **0**, waarmee u de time-out uitschakelt.

Aggregation Window Size (Grootte aggregatievenster) Met deze optie bepaalt u het maximumaantal pakketten dat wordt verzonden zonder ACK's te krijgen. Het bereik is **0** tot **64**. De standaardinstelling is **64**.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Wireless (WLAN) > Advanced Wireless Settings (Geavanceerde instellingen WLAN)

Configureer de geavanceerde draadloze functies van de bridge. Deze instellingen dienen alleen door ervaren beheerders te worden aangepast, omdat bij onjuiste instellingen de prestaties van het draadloze netwerk kunnen afnemen.



OPMERKING
De instellingen in het scherm *Advanced Wireless Settings* (Geavanceerde instellingen WLAN) zijn alleen geschikt voor geavanceerde gebruikers.

Advanced Wireless Settings (Geavanceerde instellingen WLAN)

Use LDPC (LDPC gebruiken) Met Low-Density Parity-Check Code (LDPC) schakelt u de foutcorrectie in of uit om het risico op gegevensverlies in kanalen met veel ruis te verlagen. Het algoritme voor het aanpassen van de snelheid heeft automatisch de LDPC-codering uitgeschakeld bij het werken op hoge PHY-snelheden (hoger dan 162). Gebruik de standaardinstelling **Yes** (Ja) om het geavanceerde LDCP-foutcorrectieschema te gebruiken. Selecteer anders **No** (Nee).

ERP Protection Type (Type ERP-beveiliging) Met deze optie configureert u de beveiliging van OFDM-pakketten ondanks de aanwezigheid van 802.11b-stations binnen het draadloze netwerk. Door RTS/CTS- of CTS2Self-pakketten met 802.11b-snelheden te versturen, laat de bridge het draadloze netwerk weten dat er OFDM-pakketten gaan worden verstuurd en beveiligt de bridge de pakketten binnen het draadloze netwerk. De RTS/CTS- en CTS2Self-pakketten veroorzaken overhead, waardoor de doorvoer mogelijk lager wordt.

De RTS/CTS-optie zorgt voor een betere dekking maar een lagere doorvoer in vergelijking met CTS2Self, omdat de RTS/CTS-optie bevestiging van het ontvangende apparaat vraagt. Gebruik de standaardinstelling **RTS/CTS** om de optie RTS/CTS te gebruiken. De optie None (Geen) kan ertoe leiden dat OFDM- en CCK-pakketten met elkaar botsen. Selecteer **None** (Geen) om de optie None (Geen) te gebruiken. Select **CTS2Self** om de optie CTS2Self te gebruiken.

11n Protection Type (Type 11n-beveiliging) Met deze optie configureert u de beveiliging van non-HT-apparaten (non-High Throughput) binnen het draadloze netwerk. Als de draadloze router (of het access point) een koppeling van een ouder non-HT-apparaat detecteert, verstuurt het vóór de gegevensoverdracht een signaal naar alle HT-apparaten zodat deze het RTS/CTS- of CTS2Self-mechanisme gebruiken. Deze functie ondersteunt ook alle standaard 802.11n-beveiligingen, inclusief MIMO.

De RTS/CTS-optie zorgt voor een betere dekking maar een lagere doorvoer in vergelijking met CTS2Self, omdat de RTS/CTS-optie bevestiging van het ontvangende apparaat vraagt. Gebruik de standaardinstelling **RTS/CTS** om de optie RTS/CTS te gebruiken. De optie None (Geen) kan ertoe leiden dat HT-pakketten en oudere pakketten met elkaar botsen. Selecteer **None** (Geen) om de optie None (Geen) te gebruiken. Select **CTS2Self** om de optie CTS2Self te gebruiken.

Percentage of maximal transmit power (Percentage van maximaal verzendvermogen) Met deze optie stelt u het percentage van het maximale verzendvermogen in vergelijking met de beperkingen van de regio in. Als de beperkingen van de regio overdrachten toestaat tot 20 dB, is het maximale verzendvermogen met een percentage van 50% 10 dB. Selecteer het percentage dat u wilt gebruiken: **12%**, **25%**, **50%** of **100%**. De standaardinstelling is **100%**.

QoS Classification Type (Type QoS-classificatie) Met deze optie stelt u 802.1D- of 802.1Q-toewijzing in van het veld IP DSCP/TOS voor WMM-prioriteiten (Background (Achtergrond), Best Effort (Beste poging), Video, Voice (Spraak)). Gebruik de standaardinstelling **802.1D** of selecteer de instelling **802.1Q**, die door sommige IPTV-streams wordt gebruikt.

Re-establish Ethernet connection when initiating wireless connection (Ethernetverbinding opnieuw tot stand brengen wanneer u draadloos verbinding maakt) Om DHCP-detectie te triggeren vanaf het apparaat dat zich achter de bridge bevindt, stelt de bridge de Ethernetverbinding tussen de bridge en het apparaat elke keer nadat een draadloze verbinding tot stand is gebracht. Als u dit wilt uitschakelen selecteert u **No** (Nee). Zo niet, behoud dan de standaardinstelling **Yes** (Ja).

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Administration (Administratie) > Management (Beheer)

Gebruik dit scherm om specifieke functies van de bridge te beheren: toegang tot het webgebaseerde hulpprogramma, back-up maken van het configuratiebestand en opnieuw opstarten.



Management (Beheer)

Toegang tot bridge

Gebruik een wachtwoord om het browsergebaseerde hulpprogramma te beveiligen.

Bridge Password (Wachtwoord van bridge) Voer een nieuw wachtwoord in voor de bridge.

Re-enter to Confirm (Voer opnieuw in ter bevestiging) Voer het wachtwoord nogmaals in om het te bevestigen.

Idle Timeout (Time-out bij inactiviteit) Er treedt een time out op bij het aanmelden na een periode van inactiviteit die u opgeeft. Het bereik is **60** tot **3600** seconden. De standaardinstelling is **600**.

Web Access (Internettoegang)

Access via Wireless (Toegang via WLAN) Als u de bridge gebruikt in een openbaar domein waarin u draadloze toegang verleent aan gastgebruikers, kunt u draadloze toegang tot het browsergebaseerde hulpprogramma van de bridge uitschakelen. U hebt dan alleen toegang tot het browsergebaseerde hulpprogramma via een bekabelde aansluiting. Houd de standaardinstelling **Enabled** (Ingeschakeld) als u draadloze toegang tot het browsergebaseerde hulpprogramma van de bridge wilt toestaan. Selecteer **Disabled** (Uitgeschakeld) als u de draadloze toegang tot het hulpprogramma wilt blokkeren.

Backup and Restore (Back-up en herstel)

Backup (Back-up) Klik op **Backup Configurations** (Back-up van configuraties maken) om een back-up te maken van het configuratiebestand van de bridge. Volg de instructies op het scherm.

Restore (Herstellen) Klik op **Browse** (Bladeren) en selecteer het configuratiebestand. Klik vervolgens op **Restore Configurations** (Configuraties herstellen).

System Reboot (Systeem opnieuw opstarten)

Reboot (Herstarten) Klik op **Start to Reboot** (Nu herstarten) om de bridge opnieuw op te starten.

Klik op **Save Settings** (Instellingen opslaan) om de wijzigingen door te voeren of klik op **Cancel Changes** (Wijzigingen annuleren) om de wijzigingen te annuleren.

Administration (Administratie) > Factory Defaults (Fabrieksinstellingen)

Met dit scherm kunt u de configuratie van de bridge terugzetten naar de fabrieksinstellingen.

Factory Defaults (Fabrieksinstellingen)

Restore All Settings (Alle instellingen herstellen) Klik op **Restore All Settings** (Alle instellingen herstellen) om de instellingen van de bridge terug te zetten naar de fabrieksinstellingen. Als u de standaardinstellingen herstelt, gaan alle door u opgeslagen instellingen verloren.



Administration (Administratie) > Upgrade Firmware (Firmware upgraden)

Gebruik dit scherm om een upgrade uit te voeren van de firmware van de bridge. Voer alleen een upgrade van de firmware uit wanneer u problemen ondervindt met de bridge of als de nieuwe firmware een functie heeft die u wilt gebruiken.



Download het firmware-upgradebestand voor de bridge van de Linksys-website, **www.linksys.com/support**, voordat u een upgrade op de firmware uitvoert.

Upgrade Firmware (Firmware upgraden)

Please select a file to upgrade the firmware (Selecteer het bestand dat de upgrade voor de firmware bevat) Klik op **Browse** (Bladeren) en selecteer het upgradebestand voor de firmware. Klik vervolgens op **Start to Upgrade** (Upgrade starten) en volg de instructies op het scherm.

Status > Bridge

De informatie over de huidige status van de bridge wordt weergeven.



Bridge-informatie

Firmware Version (Firmwareversie) De huidige firmwareversie van de bridge wordt weergegeven.

Local Network (Lokaal netwerk)

Local MAC Address (Lokaal MAC-adres) Dit is het MAC-adres van de bridge zoals dit wordt weergegeven in uw lokale Ethernetnetwerk.

IP Address (IP-adres) Dit is het IP-adres van de bridge zoals dit wordt weergegeven in uw lokale Ethernetnetwerk.

Subnet Mask (Subnetmasker) Het subnetmasker dat is geconfigureerd voor uw lokale netwerk wordt weergegeven.

Status > Wireless (WLAN)

Hier wordt informatie over uw draadloze netwerk weergegeven.



Wireless (WLAN)

Link Status (Verbindingsstatus) De status van de verbinding met uw draadloze netwerk wordt weergegeven.

MAC Address (MAC-adres) Dit is het MAC-adres van de bridge zoals dit wordt weergegeven in uw lokale draadloze netwerk.

Network Name (SSID) (Netwerknaam (SSID)) De naam van het draadloze netwerk of SSID wordt weergegeven.

BSSID Het draadloze MAC-adres van de aangesloten draadloze router (of het aangesloten access point) wordt weergegeven.

Radio Band (Radioband) De radioband van uw draadloze netwerk wordt weergegeven.

Channel Width (Kanaalbreedte) De kanaalbreedte in MHz die door uw draadloze netwerk wordt gebruikt, wordt weergegeven.

Wide Channel (Breed kanaal) Afhankelijk van de kanaalinstellingen van uw netwerkrouter wordt de instelling voor Breed kanaal weergegeven. Als u Wide - 40MHz Channel (Breed - kanaal 40 MHz) hebt geselecteerd als instelling voor de radioband van de router of voor Breed kanaal, is deze instelling uw primair Wireless-N kanaal.

Standard Channel (Standaardkanaal) De instelling voor het standaardkanaal wordt weergegeven. Als u Wide - 40MHz Channel (Breed - kanaal 40 MHz) hebt geselecteerd als instelling voor de radioband van de router of voor breed kanaal, is het standaardkanaal een secundair kanaal voor Wireless-N.

Bit Rate (Bitsnelheid) De snelheid van de gegevensoverdracht wordt weergegeven.

Signal (Signaal) Het percentage van de signaalsterkte wordt weergegeven. 100% is het sterkst mogelijke signaal, 0% is het zwakst mogelijke signaal.

Security (Beveiliging) Hier ziet u de beveiligingsmethode van uw draadloze netwerk.

Probleemoplossing

WES610N/WET610N

Uw computer of een ander bekabeld Ethernetapparaat kan niet communiceren met de draadloze router.

1. Open het browsergebaseerde hulpprogramma van de bridge.
2. Controleer in het scherm *Basic Wireless Settings* (Standaardinstellingen WLAN) of de netwerknaam (SSID) overeenkomt met de naam van uw draadloze netwerk.
3. Controleer of de beveiligingsinstellingen (WPA, WPA2 of WEP) overeenkomen met de beveiligingsinstellingen van uw draadloze netwerk.

Het IP-adres van de bridge dient te worden gewijzigd.

Als de bridge is aangesloten op een netwerk met een DHCP-server (meestal de netwerkrouter), wijst de DHCP-server een IP-adres toe aan de bridge. Als er geen DHCP-server is, gebruikt de bridge het standaard vaste IP-adres, **169.254.1.250**.

Als u wilt dat de bridge altijd een vast IP-adres gebruikt, volgt u onderstaande instructies:

1. Open het browsergebaseerde hulpprogramma van de bridge.
2. Klik op het tabblad **Network Setup** (Netwerkinstellingen).
3. Selecteer *Static IP* (Vast IP-adres) uit het vervolgkeuzemenu **Network Connection Type** (Type netwerkverbinding).
4. Vul de velden *Static IP Address* (Vast IP-adres), *Subnet Mask* (Subnetmasker) en *Default Gateway* (Standaardgateway) in.
5. Klik vervolgens op **Save Settings** (Instellingen opslaan).

De computer met bridge of een ander bekabeld Ethernetapparaat communiceert niet met een ander draadloos apparaat (zoals een computer of printer).

Controleer het volgende:

- Controleer of het draadloze apparaat zich op hetzelfde draadloze netwerk bevindt als de computer of het andere bekabelde Ethernetapparaat die/dat is verbonden met de bridge.
- Controleer of dezelfde netwerknaam (SSID) wordt gebruikt voor alle apparaten op het draadloze netwerk.
- Controleer of alle apparaten zich op hetzelfde IP-netwerk bevinden en compatibele IP-adressen gebruiken.

Het browsergebaseerde hulpprogramma accepteert uw wachtwoord niet.

Controleer het volgende:

- Het wachtwoord is hoofdlettergevoelig. Controleer bij het invoeren van het wachtwoord of u hoofdletters moet gebruiken.
- Als u uw wachtwoord bent vergeten, kunt u de fabrieksinstellingen van de bridge herstellen.

 Houd de knop **Reset** ongeveer vijf seconden ingedrukt; het wachtwoord wordt hersteld naar de fabrieksinstellingen: **admin**. Ook alle overige instellingen van de bridge worden naar de fabrieksinstellingen hersteld. (Voor toegang tot het browsergebaseerde hulpprogramma voert u **admin** in het veld *Password* (Wachtwoord) in.)

Als u wijzigingen hebt doorgevoerd via het browsergebaseerde hulpprogramma, worden de nieuwe instellingen niet op het scherm weergegeven.

Klik in uw webbrowser op **Refresh** (Vernieuwen). Als de instellingen niet worden weergegeven, volgt u deze instructies:

1. Koppel de netstroomadapter los van de bridge.
2. Wacht vijf seconden en sluit de netstroomadapter weer aan op de bridge.
3. Klik in uw webbrowser op **Refresh** (Vernieuwen).

WEB
Raadpleeg de website van Linksys op **www.linksys.com/support** als uw vragen niet zijn behandeld in deze bijlage

Specificaties

WES610N

Model:	WES610N
Standaarden	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED's	Voeding, Ethernet, Wi-Fi Protected Setup™, Draadloos, individuele Ethernetverbinding en activiteit
Poorten	Ethernet (4), Voeding
Knoppen	Reset, Wi-Fi Protected Setup
Type bekabeling	CAT 5e
Antennes	3 (intern)
Antenne-connectortype	N.v.t.
Afneembaar (Ja/Nee)	Nee
Modulaties	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Signaalsterkte (EIRP) in dBm	802.11a: 15 dBm (normaal) bij 54 Mbps 802.11b: 19 dBm (normaal) bij 11 Mbps 802.11g: 16 dBm (normaal) bij 54 Mbps 802.11n (2,4 GHz): 18 dBm (normaal) bij MCS15 802.11n (5 GHz): 16 dBm (normaal) bij MCS15
Ontvangstgevoeligheid	802.11a: -72 dBm (normaal) bij 54 Mbps 802.11b: -85 dBm (normaal) bij 11 Mbps 802.11g: -73 dBm (normaal) bij 54 Mbps 802.11n (20 MHz): -75 dBm (normaal) bij MCS15 802.11n (40 MHz): -69 dBm (normaal) bij MCS15
Antenneversterking in dBi	1
WLAN-beveiliging	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Beveiligingssleutelbits	Max. 128-bits versleuteling

Omgeving

Afmetingen	177 x 128 x 68 mm
Gewicht	295 g
Certificering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Voeding	12 V, 1 A
Bedrijstemperatuur	0 tot 40 °C
Opslagtemperatuur	-20 tot 60 °C
Bedrijfsvochtigheid	10 tot 85%, niet-condenserend
Opslagvochtigheid	5 tot 90%, niet-condenserend

Specificaties kunnen zonder kennisgeving worden gewijzigd.

WET610N

Model	WET610N
Standaarden	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED's	Voeding, Ethernet, Wi-Fi Protected Setup™, Draadloos
Poorten	Ethernet, Voeding
Knoppen	Reset, Wi-Fi Protected Setup
Type bekabeling	CAT 5e
Antennes	3 (intern)
Antenne-connectortype	N.v.t.
Afneembaar (Ja/Nee)	Nee
Modulaties	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Signaalsterkte (EIRP) in dBm	802.11a: 15 dBm (normaal) bij 54 Mbps 802.11b: 18 dBm (normaal) bij 11 Mbps 802.11g: 16 dBm (normaal) bij 54 Mbps 802.11n: 12 dBm (normaal) bij 130 Mbps (HT20), 270 Mbps (HT40)
Ontvangstgevoeligheid	802.11a: -72 dBm (normaal) bij 54 Mbps 802.11b: -85 dBm (normaal) bij 11 Mbps 802.11g: -73 dBm (normaal) bij 54 Mbps 802.11n: -70 dBm (normaal) bij MCS15/2,4 GHz, -69 dBm (normaal) bij MCS15/5,0 GHz
Antenneversterking in dBi	1
WLAN-beveiliging	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Beveiligingssleutelbits	Max. 128-bits versleuteling

Omgeving

Afmetingen	145 x 106 x 52 mm
Gewicht	159 g
Certificering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Voeding	12 V, 1 A
Bedrijstemperatuur	0 tot 40 °C
Opslagtemperatuur	-20 tot 60 °C
Bedrijfsvochtigheid	10 tot 85%, niet-condenserend
Opslagvochtigheid	5 tot 90%, niet-condenserend

Specificaties kunnen zonder kennisgeving worden gewijzigd.

Linksys.com/support

Cisco, het Cisco-logo en Linksys zijn handelsmerken of gedeponeerde handelsmerken van Cisco en/of zijn dochterondernemingen in de Verenigde Staten en bepaalde andere landen.
Ga naar www.cisco.com/go/trademarks voor een lijst met handelsmerken van Cisco. Alle andere handelsmerken die in dit document worden genoemd, zijn eigendom van hun respectieve eigenaren.

© 2011 Cisco en/of zijn dochterondernemingen. Alle rechten voorbehouden.

3425-01249



Brukerhåndbok

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

Innhold

Produktoversikt

Lampepanel 2
Portpanel 3

Sjekkliste for trådløs sikkerhet

Endre standardnavnet eller SSIDen for det trådløse nettverket 4
Endre standardpassordet 4
Aktivere MAC-adressefiltrering 4
Aktivere kryptering 4
Generelle retningslinjer for nettverkssikkerhet 4
Flere sikkerhetstips 5

Avansert konfigurasjon

Slik får du tilgang til det webbaserte verktøyet. 6
Setup (Konfigurasjon) > Basic Setup (Grunnleggende konfigurasjon) 7
Language (Språk) 7
Network Setup (Nettverkskonfigurasjon) 7
Wireless (Trådløst) > Basic Wireless Settings (Grunnleggende trådløsinnstilinger) 7
Basic Wireless Settings (Grunnleggende trådløsinnstilinger) 8
Wireless Security (Trådløs sikkerhet) 8
Wi-Fi Protected Setup 9
Wireless (Trådløs) > Wireless Network Site Survey (Områdeundersøkelse for trådløst nettverk) 10
Wireless Network Site Survey (Områdeundersøkelse for trådløst nettverk) 10
Wireless (Trådløst) > WMM® 11
WMM 12
Wireless (Trådløst) > Advanced Wireless Settings (Avanserte trådløsinnstilinger) 13
Advanced Wireless (Avansert trådløst) 14
Administration (Administrasjon) > Management (Styring) . . . 14
Management (Styring) 14
Administration (Administrasjon) > Factory Defaults (Fabrikkstandarder) 15
Factory Defaults (Fabrikkstandarder) 15
Administration (Administrasjon) > Upgrade Firmware (Oppgrader fastvare) 15
Upgrade Firmware (Oppgrader fastvare) 15
Status > Bridge (Bro) 15
Bridge Information (Broinformasjon) 16
Local Network (Lokalt nettverk) 16
Status > Wireless (Trådløst) 16
Wireless (Trådløst) 16

Feilsøking

WES610N/WET610N 17

Spesifikasjoner

WES610N 18
WET610N 19

Produktoversikt

Takk for at du valgte Linksys Dual-Band N Entertainment Bridge. Broen kan ikke koble kablede Ethernet-enheter til det trådløse nettverket. Broen er basert på Wireless-N med doble bånd og er dermed kompatibel med alle rutere eller tilgangspunkt av typen Wireless-N, -G, -A eller -B. Følg trinnene i CD-mappen for installasjon første gang. Bruk det enkle, webbaserte verktøyet til å konfigurere avanserte innstillinger.

Lampepanel



WES610N WET610N

Wireless (Trådløst) (blå) Trådløst-lampen lyser når det finnes en trådløs tilkobling. Lampen blinker når broen sender eller mottar data aktivt data via det trådløse nettverket.

Knappen Wi-Fi Protected Setup Hvis nettverksruteren støtter Wi-Fi Protected Setup og bruker WPA- eller WPA2-sikkerhet, kan du bruke Wi-Fi Protected Setup til å koble til broen automatisk. Hvis du vil bruke Wi-Fi Protected Setup, kan du se "Wireless (Trådløst) > Basic Wireless Settings (Grunnleggende trådløsinnstilinger)" på side 7.

Lampe for Wi-Fi Protected Setup (blå/gul) Lampen blinker blått i to minutter under Wi-Fi Protected Setup. Den lyser kontinuerlig blått når trådløs sikkerhet er aktivert. Hvis det oppstår en feil under Wi-Fi Protected Setup-prosessen, lyser lampen kontinuerlig gult. Kontroller at nettverksruteren støtter Wi-Fi Protected Setup. Vent til LED-lampen er slått av, og forsøk igjen.

Ethernet (blå) Ethernet-lampen lyser når det finnes en kablet tilkobling. Lampen blinker når broen sender eller mottar data aktivt data via Ethernet-porten(e).

Power (Strøm) (blå) Strømlampen lyser så lenge broen er slått på.

Portpanel



WES610N WET610N

Ethernet Ethernet-porten(e) kobler broen til en datamaskin eller en annen Ethernet-nettverksenhet. WES610N har fire porter, og WET610N har én port.

Reset (Tilbakestill) Det er to måter du kan tilbakestille broen til fabrikkstandardene på. Du kan trykke på og holde nede knappen Reset (Tilbakestill) i ca. fem sekunder, eller du kan gjenopprette standardene fra Administration (Administrasjon) > Factory Defaults (Fabrikkstandarder) i det webbaserte verktøyet for broen. WES610N har en tilbakestillingsknapp på undersiden, og WET610N har en tilbakestillingsknapp på det bakre portpanelet.

Power (Strøm) Strømporten kobler broen til den tilhørende strømadapteren.

Sjekkliste for trådløs sikkerhet

Trådløse nettverk er brukervennlige og enkle å installere, og hjem med Internett-tilgang med høy hastighet tar dem derfor stadig oftere i bruk. Ettersom trådløse nettverk fungerer ved å sende informasjon via radiobølger, kan de være mer utsatte for inntrengere enn et tradisjonelt kablet nettverk. I likhet med signaler fra mobiltelefoner eller trådløse telefoner kan også signaler fra det trådløse nettverket bli fanget opp. Ettersom du ikke fysisk kan hindre noen i å koble til det trådløse nettverket, må du utføre noen tilleggstrinn for å sikre nettverket.

Endre standardnavnet eller SSIDen for det trådløse nettverket

Trådløse enheter har et standardnavn eller en SSID (Service Set Identifier) for det trådløse nettverket som er angitt på fabrikken. Dette er navnet på det trådløse nettverket og kan bestå av opptil 32 tegn. Trådløse produkter fra Linksys bruker **linksys** som standardnavn for trådløse nettverk. Du bør endre navnet på det trådløse nettverket til noe unikt, slik at du skiller ditt eget trådløse nettverk fra andre trådløse nettverk som kanskje finnes i nærheten. Du må imidlertid ikke bruke personlige opplysninger (for eksempel personnummer), ettersom disse opplysningene kan være synlige for alle som søker etter trådløse nettverk.

Endre standardpassordet

For trådløse produkter, for eksempel tilgangspunkter og rutere, vil du bli bedt om å angi et passord når du vil endre innstillingene. Et standardpassord blir angitt på fabrikken for disse enhetene. Standardpassordet for Linksys er **admin**. Hackere kjenner til disse standardverdiene og vil kanskje prøve å bruke dem for å få tilgang til den trådløse enheten og endre nettverksinnstillingene. Du kan unngå slike uautoriserte endringer ved å tilpasse enhetspassordet slik at det er vanskelig å gjette det.

Aktivere MAC-adressefiltrering

Med Linksys-rutere har du muligheten til å aktivere MAC-adressefiltrering (Media Access Control). MAC-adressen er en unik serie med tall og bokstaver som er tilordnet til hver eneste nettverksenhet. Når MAC-adressefiltrering er aktivert, blir det bare gitt tilgang til det trådløse nettverket til trådløse enheter med spesifikke MAC-adresser. Du kan for eksempel angi MAC-adressen for hver datamaskin i hjemmet, slik at bare disse datamaskinene kan få tilgang til det trådløse nettverket.

Aktivere kryptering

Kryptering beskytter data som overføres via et trådløst nettverk. Wi-Fi Protected Access (WPA/WPA2) og Wired Equivalent Privacy (WEP) tilbyr ulike sikkerhetsnivåer for trådløs kommunikasjon.

Et nettverk som er kryptert med WPA/WPA2, er sikrere enn et nettverk som er kryptert med WEP, ettersom WPA/WPA2 bruker kryptering med dynamiske nøkler. Du kan beskytte informasjonen som sendes gjennom luftbølgene, ved å aktivere det høyeste krypteringsnivået nettverksutstyret støtter.

WEP er en eldre krypteringsstandard og er kanskje det eneste alternativet som er tilgjengelig på enkelte eldre enheter som ikke støtter WPA.

Generelle retningslinjer for nettverkssikkerhet

Sikkerhet for trådløse nettverk er nytteløst hvis det underliggende nettverket ikke er sikkert.

- Beskytt alle datamaskiner i nettverket med passord, og beskytt sensitive filer med individuelle passord.
- Endre passordene regelmessig.
- Installer antivirusprogrammer og personlige brannmurprogrammer.
- Deaktiver fildeling (maskin-til-maskin). Enkelte programmer kan åpne fildeling uten at du samtykker i det og/eller vet om det.

Flere sikkerhetstips

- Hold trådløse rutere, tilgangspunkter eller gatewayer unna yttervegger og vinduer.
- Slå av trådløse rutere, tilgangspunkter eller gatewayer når de ikke brukes (om natten, i ferier).
- Bruk sterke passord som inneholder minst åtte tegn. Kombiner bokstaver og tall for å unngå å bruke vanlige ord som kan slås opp i ordbøker.

Avansert konfigurasjon

Når du har konfigurert broen ved å følge trinnene i CD-mappen, er broen klar for bruk. Hvis du vil endre de avanserte innstillingene, kan du imidlertid bruke det webbaserte verktøyet for broen. Dette kapittelet beskriver alle sidene i det webbaserte verktøyet og de viktigste funksjonene på hver side. Du kan få tilgang til verktøyet via en webleser på en datamaskin som er koblet til broen.

Det webbaserte verktøyet har disse hovedkategoriene: Setup (Konfigurasjon), Wireless (Trådløst), Administration (Administrasjon) og Status. Når du klikker på en av hovedkategoriene, blir flere kategorier tilgjengelige.

Slik får du tilgang til det webbaserte verktøyet

Bruk en webleser til å få tilgang til det webbaserte verktøyet.

Hvis broen er koblet til et nettverk via en DHCP-server (vanligvis nettverksruteren), vil broen hente IP-adressen fra DHCP-serveren. Hvis det ikke finnes noen DHCP-server, vil broen bruke standard statisk IP-adresse, som er **169.254.1.250**. (Hvis du angir en permanent statisk IP-adresse i broen via det webbaserte verktøyet, angir du denne statiske IP-adressen i stedet.)

MERK

Hvis du ikke kjenner broens IP-adresse, finner du den i DHCP-klientens tabell for ruteren. (Se dokumentasjonen for ruteren.)

Hvis du ikke finner broens IP-adresse, kan du tilbakestille broen. Trykk på knappen **Reset** (Tilbakestill) på broen i ca. fem sekunder, med en utbrettet binders. Dette vil tilbakestille broen til fabrikkstandardene. Broen vil be om en IP-adresse fra DHCP-serveren (vanligvis nettverksruteren). Hvis ingen DHCP-server blir funnet, vil broen bruke standard statisk IP-adresse, som er **169.254.1.250**, til den finner en DHCP-server og får tilordnet en dynamisk IP-adresse.

Hvis broen ikke er knyttet til en ruter og bruker fabrikkstandardene, kobler du en datamaskin til broen via en Ethernet-tilkobling for å få tilgang til det webbaserte verktøyet. Du må konfigurere Ethernet-tilkoblingen på datamaskinen med en statisk IP-adresse og delnettmaske.

IP-adressen for Ethernet-kortet bør settes til en angitt IP-adresse.

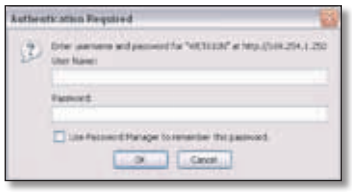
1. I feltet *IP address* (IP-adresse) angir du **169.254.x.y** (x skal byttes ut med et tall mellom 1 og 254, og y skal byttes ut med et tall mellom 0 og 255).
2. I feltet *Subnet mask* (Delnettmaske) angir du **255.255.0.0**.

MERK

Trinnene for tilordning av en statisk IP-adresse til Ethernet-kortet på datamaskinen varierer avhengig av operativsystem. Du finner instruksjoner i hjelpedokumentasjonen for operativsystemet du bruker.

Når du har tilordnet en statisk IP-adresse til Ethernet-kortet, starter du webleseren og angir kortets IP-adresse (standardinnstillingen er **169.254.1.250**) i feltet *Address* (Adresse). Trykk på **Enter**.

Et skjermbilde med en passordforespørsel vises. (Brukere med et annet operativsystem enn Windows XP vil se et lignende skjermbilde.) La feltet *Brukernavn* stå tomt. Angi passordet du opprettet i konfigurasjonsveiviseren. Hvis du ikke opprettet et nytt passord, bruker du standardpassordet **admin**. (Du kan angi et nytt passord i skjermbildet *Administration* (Administrasjon) > *Management* (Styring). Klikk på **OK** for å fortsette.



MERK

Hvis skjermbildet med passordforespørsel ikke vises, venter du to minutter og prøver på nytt.

Setup (Konfigurasjon) > Basic Setup (Grunnleggende konfigurasjon)

Det første skjermbildet som vises, er *Basic Setup* (Grunnleggende konfigurasjon). Bruk dette skjermbildet til å endre språk for det webbaserte verktøyet, eller til å endre innstillingene for broens kablede Ethernet-nettverk.





Language (Språk)

Language (Språk) Dette brukes til å angi språket som vises i det webbaserte verktøyet. Velg ønsket språk på hurtigmenyen.

Network Setup (Nettverkskonfigurasjon)

Denne delen fastsetter om broens IP-adresse er hentet automatisk fra en DHPC-server, for eksempel nettverksruteren (Automatic Configuration (Automatisk konfigurasjon) - DHCP) eller angitt manuelt (Static IP (Statisk IP)).

Bridge IP (Bro-IP) Hvis nettverket har en DHCP-server, for eksempel nettverksruteren, som tilordner IP-adresser til nettverksenhetene, beholder du standarden, **Automatic Configuration** (Automatisk konfigurasjon) **- DHCP**. Broen vil be om en IP-adresse fra DHCP-serveren (vanligvis nettverksruteren). Hvis ingen DHCP-server blir funnet, vil broen bruke standard statisk IP-adresse, som er **169.254.1.250**, til den finner en DHCP-server og får tilordnet en dynamisk IP-adresse.

Hvis du vil angi en permanent statisk IP-adresse for broen, velger du **Static IP** (Statisk IP).

Hvis du velger Static IP (Statisk IP), fyller du ut følgende felt:

- **Static IP Address** (Statisk IP-adresse) Angi en unik IP-adresse som skal brukes til å få tilgang til det webbaserte verktøyet.
- **Subnet Mask** (Delnettmaske) Angi delnettmasken for det kablede nettverket.
- **Default Gateway** (Standardgateway) Angi IP-adressen for standardgatewayen for nettverket (i de fleste tilfeller er dette ruteren).

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Wireless (Trådløst) > Basic Wireless Settings (Grunnleggende trådløsinnstilinger)

Bruk skjermbildet *Basic Wireless Settings* (Grunnleggende trådløsinnstillinger) til å konfigurere innstillingene for broens trådløsnett og sikkerhet.

Broinnstillingene kan konfigureres på to måter: manuelt eller med Wi-Fi Protected Setup. Wi-Fi Protected Setup er en funksjon som gjør det enkelt å konfigurere trådløse nettverk. Hvis nettverksruteren støtter Wi-Fi Protected Setup og bruker WPA- eller WPA2-sikkerhet, kan du bruke Wi-Fi Protected Setup til automatisk tilkobling av broen.

Configuration View (Konfigurasjonsvisning) Hvis du vil konfigurere det trådløse nettverket manuelt, velger du **Manual** (Manuelt). Se **Basic Wireless Settings** (Grunnleggende trådløsinnstilinger), **side 8**. Hvis du vil bruke Wi-Fi Protected Setup, velger du **Wi-Fi Protected Setup**. Se **Wi-Fi Protected Setup**, **side 9**.

Basic Wireless Settings (Grunnleggende trådløsinnstilinger)



Network Name (SSID) (Nettverksnavn (SSID)) SSIDen er nettverksnavnet som deles av alle punktene i et trådløst nettverk. SSIDen må være identisk for alle enheter i det trådløse nettverket. Den skiller mellom store og små bokstaver og kan maksimalt inneholde 32 tegn (bruk hvilke som helst tegn på tastaturet). Kontroller at denne innstillingen samsvarer med innstillingen på den trådløse ruteren eller tilgangspunktet. For ekstra sikkerhet bør du endre standard SSID (**linksys**) til et unikt navn.

Wireless Security (Trådløs sikkerhet)

Broen støtter følgende alternativer for trådløs sikkerhet: WPA Personal, WPA2 Personal og WEP. WPA (Wi-Fi Protected Access) og WPA2 er sterkere sikkerhetsmetoder enn WEP (Wired Equivalent Privacy). Hvis du vil ha mer informasjon om trådløs sikkerhet, kan du se "Sjekkliste for trådløs sikkerhet", side 4.

Security Mode (Sikkerhetsmodus)

Velg sikkerhetsmetode for det trådløse nettverket. Hvis du ikke vil bruke trådløs sikkerhet, beholder du standardinnstillingen **Disabled** (Deaktivert).

MERK
Husk at alle enheter i det trådløse nettverket MÅ bruke samme sikkerhetsmetode og passord/nøkkel, elles kan de ikke kommunisere med hverandre.

WPA Personal

WPA er en sikkerhetsstandard som er sterkere enn WEP-kryptering.



Encryption (Kryptering) WPA støtter krypteringsmetoden TKIP, med dynamiske krypteringsnøkler.

Passphrase (Passord) Angi nøkkelen som deles av broen og den trådløse ruteren eller tilgangspunktet. Den må bestå av mellom 8 og 63 tegn.

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

WPA2 Personal

WPA2 er en sikrer og mer avansert versjon av WPA.



Encryption (Kryptering) WPA2 støtter to krypteringsmetoder, TKIP og AES, med dynamiske krypteringsnøkler. Velg krypteringsmetoden, **AES** eller **TKIP or (eller) AES**. Standardvalget er **AES**.

Passphrase (Passord) Angi nøkkelen som deles av broen og den trådløse ruteren eller tilgangspunktet. Den må bestå av mellom 8 og 63 tegn.

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

WEP

WEP er en enkel krypteringsmetode og ikke like sikker som WPA eller WPA2.



Encryption (Kryptering) Velg et nivå for WEP-kryptering, **40/64 biter (10 heksadesimaler)** eller **104/128 biter (26 heksadesimaler)**. Standardverdien er **40/64 biter (10 heksadesimaler)**.

Key 1 (Nøkkel 1) Angi WEP-nøkkelen for nettverket.

Tx Key (Overføringsnøkkel) **Key 1** (Nøkkel 1) er overføringsnøkkelen som brukes av broen.

Authentication (Godkjenning) Standardinnstillingen er **Auto** (Automatisk), som gir deg muligheten til å bruke godkjenning av typen Open System (Åpent system) eller Shared Key (Delt nøkkel). Velg **Open** (Åpent) hvis du vil bruke åpen systemgodkjenning. Avsenderen og mottakeren bruker ikke en WEB-nøkkel til godkjenning. Velg **Shared** (Delt) hvis du vil bruke godkjenning med delt nøkkel. Avsenderen og mottakeren bruker en WEB-nøkkel til godkjenning.

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Wi-Fi Protected Setup

Det finnes to tilgjengelige metoder. Bruk metoden som gjelder for ruteren du konfigurerer.





Metode nr. 1

Bruk denne metoden hvis ruteren har en knapp for Wi-Fi Protected Setup.

1. Klikk eller trykk på knappen **Wi-Fi Protected Setup** på ruteren.
2. I løpet av to minutter må du klikke på knappen **Wi-Fi Protected Setup** i skjermbildet *Wi-Fi Protected Setup* på broen.
3. Når broen er konfigurert, klikker du på **Close** (Lukk).

Skjermbildet *Wi-Fi Protected Setup* viser koblingsstatusen, nettverksnavnet (SSID) og sikkerhetsmetoden.

Metode nr. 2

Bruk denne metoden hvis ruteren ber om PIN-koden fra broen.

1. I **skjermbildet** *Wi-Fi Protected Setup* på ruteren angir du PIN-koden i **skjermbildet** *Wi-Fi Protected Setup* på broen. Klikk deretter på **Register** (Registrer) eller den passende knappen. (PIN-koden finner du også på etiketten på undersiden av broen.)
2. I **skjermbildet** *Wi-Fi Protected Setup* på broen klikker du på **OK**.
3. Når broen er konfigurert, klikker du på **Close** (Lukk).

Skjermbildet *Wi-Fi Protected Setup* viser koblingsstatusen, nettverksnavnet (SSID) og sikkerhetsmetoden.

Wireless (Trådløs) > Wireless Network Site Survey (Områdeundersøkelse for trådløst nettverk)

Klikk på kategorien **Wireless Network Site Survey** (Områdeundersøkelse for trådløst nettverk) for å starte en områdeundersøkelse. Skjermbildet *Wireless Network Site Survey* (Områdeundersøkelse for trådløst nettverk) viser de trådløse nettverkene broen finner.



Wireless Network Site Survey (Områdeundersøkelse for trådløst nettverk)

Number of Wireless Networks (Antall trådløse nettverk) Antallet trådløse nettverk broen finner, vises.

Select (Velg) Du kobler til et trådløst nettverk ved å klikke på **Select** (Velg). Klikk deretter på **Connect** (Koble til).

Wireless Network Name (Navn på trådløst nettverk) Nettverksnavnet eller SSIDen for det trådløse nettverket vises.

GHz Radiobåndet for det trådløse nettverket vises.

Signal Signalstyrken i prosent vises. 100% er den sterkeste signalstyrken som er mulig, og 0% er den svakeste styrken som er mulig.

Security (Sikkerhet) Hvis nettverket støtter Wi-Fi Protected Setup, vises ikonet Wi-Fi Protected Setup . Sikkerhetsmetoden som brukes i det trådløse nettverket, vises.

Klikk på **Refresh** (Oppdater) for å oppdatere informasjonen på skjermen.

Når du har valgt et nettverk, klikker du på **Connect** (Koble til). Et nytt skjermbilde vises. Følg instruksjonene for sikkerhetsmetoden for nettverket.

WPA



Network Name (SSID) (Nettverksnavn (SSID)) Navnet på nettverket du valgte, vises automatisk.

Security Mode (Sikkerhetsmodus) WPA Personal vises automatisk.

Encryption (Kryptering) WPA støtter krypteringsmetoden TKIP, med dynamiske krypteringsnøkler.

Passphrase (Passord) Angi nøkkelen som deles av broen og den trådløse ruteren eller tilgangspunktet. Den må bestå av mellom 8 og 63 tegn.

Klikk på **Refresh** (Oppdater) for å oppdatere informasjonen på skjermen.

Når du har angitt sikkerhetsinnstillingene, klikker du på **Connect** (Koble til).

WPA2



Network Name (SSID) (Nettverksnavn (SSID)) Navnet på nettverket du valgte, vises automatisk.

Security Mode (Sikkerhetsmodus) WPA2 Personal vises automatisk.

Encryption (Kryptering) WPA2 støtter to krypteringsmetoder, TKIP og AES, med dynamiske krypteringsnøkler. Velg krypteringsmetoden, **AES** eller **TKIP or (eller) AES**.

Passphrase (Passord) Angi nøkkelen som deles av broen og den trådløse ruteren eller tilgangspunktet. Den må bestå av mellom 8 og 63 tegn.

Klikk på **Refresh** (Oppdater) for å oppdatere informasjonen på skjermen.

Når du har angitt sikkerhetsinnstillingene, klikker du på **Connect** (Koble til).

WEP



Network Name (SSID) (Nettverksnavn (SSID)) Navnet på nettverket du valgte, vises automatisk.

Security Mode (Sikkerhetsmodus) WEP vises automatisk.

Encryption (Kryptering) Velg et WEP-krypteringsnivå, **40/64 biter (10 heksadesimaler)** eller **104/128 biter (26 heksadesimaler)**.

Key 1 (Nøkkel 1) Angi WEP-nøkkelen for nettverket.

Tx Key (Overføringsnøkkel) **Key 1** (Nøkkel 1) er overføringsnøkkelen som brukes av broen.

Authentication (Godkjenning) Standardinnstillingen er **Auto** (Automatisk), som gir deg muligheten til å bruke godkjenning av typen Open System (Åpent system) eller Shared Key (Delt nøkkel). Velg **Open** (Åpent) hvis du vil bruke åpen systemgodkjenning. Avsenderen og mottakeren bruker ikke en WEB-nøkkel til godkjenning. Velg **Shared** (Delt) hvis du vil bruke godkjenning med delt nøkkel. Avsenderen og mottakeren bruker en WEB-nøkkel til godkjenning.

Klikk på **Refresh** (Oppdater) for å oppdatere informasjonen på skjermen.

Når du har angitt sikkerhetsinnstillingene, klikker du på **Connect** (Koble til).

Wireless (Trådløst) > WMM®

Konfigurer innstillingene for Wireless MultiMedia (WMM). WMM gir pakker prioritet avhengig av den tilhørende tilgangsmodusen (trafikktypen): Background (Bakgrunn), Best Effort (Beste innsats), Video eller Voice (Tale). Disse innstillingene bør bare endres av en erfaren administrator fordi feil innstillinger kan redusere trådløsytelsen.



MERK
Innstillingene i skjermbildet *WMM* er bare utformet for avanserte brukere.

WMM

Access Mode (Tilgangsmodus)

Du kan tilordne ulike innstillinger til de fire tilgjengelige tilgangsmodiene. Velg modusen du vil konfigurere: **Background** (Bakgrunn), **Best Effort** (Beste innsats), **Video** eller **Voice** (Tale). Følg instruksjonene for modusen du velger.

Background (Bakgrunn)

Use Aggregation (Bruk aggregering) Dette alternativet definerer om MAC-laget (Media Access Control) vil definere en ADDBA-økt (Add Block Acknowledgement). Standardinnstillingen er **No** (Nei). Velg **Yes** (Ja) hvis du vil aktivere dette alternativet.

Accept Aggregation (Godta aggregering) Dette alternativet definerer om MAC-laget vil godta en ADDBA-forespørsel. Standardinnstillingen er **Yes** (Ja). Velg **No** (Nei) hvis du vil deaktivere dette alternativet.

Max. Number of Packets in Aggregation (Maks. antall pakker i aggregering) Dette alternativet definerer det maksimale antallet pakker (underrammer) i aggregeringen. Området er **0** til **7**. Standardinnstillingen er **7**.

Max. Aggregation Size (Maks. aggregeringsstørrelse) Dette alternativet definerer den maksimale størrelsen på aggregeringen (i byte). Området er **0** til **16 000**. Standardinnstillingen er **12 000**.

Timeout Internal (Internt tidsavbrudd) Dette alternativet definerer tidsavbruddsperioden der aggregeringen skal lukkes, med et "lukkevilkår" før tidtakeren lukker den. Området er **0** til **100** ms. Standardinnstillingen er **3**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i aggregering) Dette alternativet definerer minimumsstørrelsen (i byte) for pakker som skal samles i aggregeringen. Området er **0** til **1 500**. Standardinnstillingen er **10**.

ADDBA Timeout (ADDBA-tidsavbrudd) Dette alternativet definerer hvor lang tid det går før ADDBA-konfigurasjonen avsluttes, hvis det ikke er noen rammeutvekslinger i denne perioden i henhold til ACK-avtalen (blokkbekreftelse). Området er **0** til **65 535** ms. Standardinnstillingen er **0**, noe som deaktiverer tidsavbruddet.

Aggregation Window Size (Størrelse på aggregeringsvindu) Dette alternativet definerer det maksimale antallet pakker som overføres uten å hente ACKer. Området er **0** til **64**. Standardinnstillingen er **64**.

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Best Effort (Beste innsats)

Use Aggregation (Bruk aggregering) Dette alternativet definerer om MAC-laget (Media Access Control) vil definere en ADDBA-økt (Add Block Acknowledgement). Standardinnstillingen er **Yes** (Ja). Velg **No** (Nei) hvis du vil deaktivere dette alternativet.

Accept Aggregation (Godta aggregering) Dette alternativet definerer om MAC-laget vil godta en ADDBA-forespørsel. Standardinnstillingen er **Yes** (Ja). Velg **No** (Nei) hvis du vil deaktivere dette alternativet.

Max. Number of Packets in Aggregation (Maks. antall pakker i aggregering) Dette alternativet definerer det maksimale antallet pakker (underrammer) i aggregeringen. Området er **0** til **10**. Standardinnstillingen er **10**.

Max. Aggregation Size (Maks. aggregeringsstørrelse) Dette alternativet definerer den maksimale størrelsen på aggregeringen (i byte). Området er **0** til **20 000**. Standardinnstillingen er **16 000**.

Timeout Internal (Internt tidsavbrudd) Dette alternativet definerer tidsavbruddsperioden der aggregeringen skal lukkes, med et "lukkevilkår" før tidtakeren lukker den. Området er **0** til **100** ms. Standardinnstillingen er **3**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i aggregering) Dette alternativet definerer minimumsstørrelsen (i byte) for pakker som skal samles i aggregeringen. Området er **0** til **1 500**. Standardinnstillingen er **10**.

ADDBA Timeout (ADDBA-tidsavbrudd) Dette alternativet definerer hvor lang tid det går før ADDBA-konfigurasjonen avsluttes, hvis det ikke er noen rammeutvekslinger i denne perioden i henhold til ACK-avtalen (blokkbekreftelse). Området er **0** til **65 535** ms. Standardinnstillingen er **0**, noe som deaktiverer tidsavbruddet.

Aggregation Window Size (Størrelse på aggregeringsvindu) Dette alternativet definerer det maksimale antallet pakker som overføres uten å hente ACKer. Området er **0** til **64**. Standardinnstillingen er **64**.

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Video

Use Aggregation (Bruk aggregering) Dette alternativet definerer om MAC-laget (Media Access Control) vil definere en ADDBA-økt (Add Block Acknowledgement). Standardinnstillingen er **Yes** (Ja). Velg **No** (Nei) hvis du vil deaktivere dette alternativet.

Accept Aggregation (Godta aggregering) Dette alternativet definerer om MAC-laget vil godta en ADDBA-forespørsel. Standardinnstillingen er **Yes** (Ja). Velg **No** (Nei) hvis du vil deaktivere dette alternativet.

Max. Number of Packets in Aggregation (Maks. antall pakker i aggregering) Dette alternativet definerer det maksimale antallet pakker (underrammer) i aggregeringen. Området er **0** til **7**. Standardinnstillingen er **7**.

Max. Aggregation Size (Maks. aggregeringsstørrelse) Dette alternativet definerer den maksimale størrelsen på aggregeringen (i byte). Området er **0** til **16 000**. Standardinnstillingen er **12 000**.

Timeout Internal (Internt tidsavbrudd) Dette alternativet definerer tidsavbruddsperioden der aggregeringen skal lukkes, med et "lukkevilkår" før tidtakeren lukker den. Området er **0** til **100** ms. Standardinnstillingen er **3**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i aggregering) Dette alternativet definerer minimumsstørrelsen (i byte) for pakker som skal samles i aggregeringen. Området er **0** til **1 500**. Standardinnstillingen er **10**.

ADDBA Timeout (ADDBA-tidsavbrudd) Dette alternativet definerer hvor lang tid det går før ADDBA-konfigurasjonen avsluttes, hvis det ikke er noen rammeutvekslinger i denne perioden i henhold til ACK-avtalen (blokkbekreftelse). Området er **0** til **65 535** ms. Standardinnstillingen er **0**, noe som deaktiverer tidsavbruddet.

Aggregation Window Size (Størrelse på aggregeringsvindu) Dette alternativet definerer det maksimale antallet pakker som overføres uten å hente ACKer. Området er **0** til **64**. Standardinnstillingen er **64**.

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Voice (Tale)

Use Aggregation (Bruk aggregering) Dette alternativet definerer om MAC-laget (Media Access Control) vil definere en ADDBA-økt (Add Block Acknowledgement). Standardinnstillingen er **Yes** (Ja). Velg **No** (Nei) hvis du vil deaktivere dette alternativet.

Accept Aggregation (Godta aggregering) Dette alternativet definerer om MAC-laget vil godta en ADDBA-forespørsel. Standardinnstillingen er **Yes** (Ja). Velg **No** (Nei) hvis du vil deaktivere dette alternativet.

Max. Number of Packets in Aggregation (Maks. antall pakker i aggregering) Dette alternativet definerer det maksimale antallet pakker (underrammer) i aggregeringen. Området er **0** til **2**. Standardinnstillingen er **2**.

Max. Aggregation Size (Maks. aggregeringsstørrelse) Dette alternativet definerer den maksimale størrelsen på aggregeringen (i byte). Området er **0** til **16 000**. Standardinnstillingen er **10 000**.

Timeout Internal (Internt tidsavbrudd) Dette alternativet definerer tidsavbruddsperioden der aggregeringen skal lukkes, med et "lukkevilkår" før tidtakeren lukker den. Området er **0** til **100** ms. Standardinnstillingen er **10**.

Min. Size of Packet in Aggregation (Min. pakkestørrelse i aggregering) Dette alternativet definerer minimumsstørrelsen (i byte) for pakker som skal samles i aggregeringen. Området er **0** til **1 500**. Standardinnstillingen er **10**.

ADDBA Timeout (ADDBA-tidsavbrudd) Dette alternativet definerer hvor lang tid det går før ADDBA-konfigurasjonen avsluttes, hvis det ikke er noen rammeutvekslinger i denne perioden i henhold til ACK-avtalen (blokkbekreftelse). Området er **0** til **65 535** ms. Standardinnstillingen er **0**, noe som deaktiverer tidsavbruddet.

Aggregation Window Size (Størrelse på aggregeringsvindu) Dette alternativet definerer det maksimale antallet pakker som overføres uten å hente ACKer. Området er **0** til **64**. Standardinnstillingen er **64**.

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Wireless (Trådløst) > Advanced Wireless Settings (Avanserte trådløsinnstilinger)

Konfigurer de avanserte trådløsinnstillingene for broen. Disse innstillingene bør bare endres av en erfaren administrator fordi feil innstillinger kan redusere trådløsytelsen.



MERK
Innstillingene i skjermbildet *Advanced Wireless Settings* (Avanserte trådløsinnstillinger) er bare utformet for avanserte brukere.

Advanced Wireless (Avansert trådløst)

Use LDPC (Bruk LDPC) LDCP (Low-Density Parity-Check Code) aktiverer eller deaktiverer feilkorrigering for å redusere sannsynligheten for datatap i kanaler med mye støy. Algoritmen for hastighetstilpasning deaktiverte automatisk LDPC-koding ved arbeid med høye PHY-hastigheter (over 162). Behold standardinnstillingen **Yes** (Ja) for å bruke det avanserte LDCP-skjemaet for feilkorrigering. Hvis ikke, klikker du på **No** (Nei).

ERP Protection Type (ERP-beskyttelsestype) Dette alternativet konfigurerer beskyttelse av OFDM-pakker til tross for at det finnes 802.11b-stasjoner i det trådløse nettverket. Ved å sende RTS-/CTS- eller CTS2Self-pakker i 802.11b-hastigheter informerer broen det trådløse nettverket om at OFDM-pakker skal overføres, og beskytter pakkene i det trådløse nettverket. RTS-/CTS- og CTS2Self-pakkene skaper tidsforbruk, noe som kan føre til lavere ytelse.

Alternativet for RTS/CTS gir bedre dekning, men lavere ytelse enn CTS2Self, ettersom alternativet for RTS/CTS inkluderer bekreftelse fra mottaksenheten. Hvis du vil bruke alternativet for RTS/CTS, beholder du standardinnstillingen, som er **RTS/CTS**. Alternativet None (Ingen) kan føre til kollisjoner mellom OFDM- og CCK-pakker. Hvis du vil bruke alternativet None (Ingen), velger du **None** (Ingen). Hvis du vil bruke alternativet for CTS2Self, velger du **CTS2Self**.

11n Protection Type (11n-beskyttelsestype) Dette alternativet konfigurerer beskyttelse mot ikke-HT-enheter (High Throughput) i det trådløse nettverket. Hvis den trådløse ruteren (eller tilgangspunktet) finner en tilknytning til en eldre ikke-HT-enhet, signaliserer den til alle HT-enhetene at mekanismene for RTS/CTS eller CTS2Self skal brukes før hver dataoverføring. Denne funksjonen støtter også alle 802.11n-standardbeskyttelser, inkludert MIMO.

Alternativet for RTS/CTS gir bedre dekning, men lavere ytelse enn CTS2Self, ettersom alternativet for RTS/CTS inkluderer bekreftelse fra mottaksenheten. Hvis du vil bruke alternativet for RTS/CTS, beholder du standardinnstillingen, som er **RTS/CTS**. Alternativet None (Ingen) kan føre til kollisjoner mellom HT-pakker og eldre pakker. Hvis du vil bruke alternativet None (Ingen), velger du **None** (Ingen). Hvis du vil bruke alternativet for CTS2Self, velger du **CTS2Self**.

Percentage of maximal transmit power (Prosent av maksimal overføringskraft) Dette alternativet angir prosentdelen av maksimal overføringskraft i forhold til de regulerende domenerestriksjonene. Hvis den regulerende domenerestriksjonen for eksempel tillater overføringer på opptil 20 dB, vil en angivelse på 50 % tillate en maksimal overføringskraft på 10 dB. Velg prosentdelen du vil bruke: **12%**, **25%**, **50%** eller **100%**. Standardinnstillingen er **100%**.

QoS Classification Type (QoS-klassifiseringstype) Dette alternativet setter 802.1D- eller 802.1Q-tilordning fra feltet IP DSCP/TOS til WMM-prioriteter (Background (Bakgrunn), Best Effects (Beste innsats), Video, Voice (Tale)). Behold standardinnstillingen, som er **802.1D**, eller velg **802.1Q**, som brukes i enkelte IPTV-avspillinger.

Re-establish Ethernet connection when initiating wireless connection (Opprett Ethernet-tilkobling på nytt ved oppretting av trådløs tilkobling) Hvis du vil utløse DHCP-søk fra enheten som ligger bak broen, vil broen tilbakestille Ethernet-koblingen mellom broen og enheten hver gang en trådløs tilkobling opprettes. Hvis du vil deaktivere denne atferden, velger du **No** (Nei). Ellers beholder du standardinnstillingen, som er **Yes** (Ja).

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Administration (Administrasjon) > Management (Styring)

Bruk dette skjermbildet til å styre spesifikke brofunksjoner: tilgang til det webbaserte verktøyet, sikkerhetskopiering av konfigurasjonsfilen og omstart.



Management (Styring)

Bridge Access (Brotilgang)

Bruk et passord til å beskytte tilgangen til det webbaserte verktøyet.

Bridge Password (Bropassord) Angi et nytt passord for broen.

Re-enter to confirm (Skriv inn på nytt for å bekrefte) Skriv inn passordet på nytt for å bekrefte det.

Idle Timeout (Tidsavbrudd ved inaktivitet) Påloggingen blir tidsavbrutt etter en periode med inaktivitet som du angir. Området er **60** til **3 600** sekunder. Standardinnstillingen er **600**.

Web Access (Webtilgang)

Access via Wireless (Trådløs tilgang) Hvis du bruker broen i et offentlig domene der du gir gjestene trådløs tilgang, kan du deaktivere trådløs tilgang til det webbaserte verktøyet for broen. Hvis du deaktiverer denne innstillingen, kan du bare få tilgang til det webbaserte verktøyet via en kablet tilkobling. Behold standardinnstillingen, som er **Enabled** (Aktivert), hvis du vil tillate trådløs tilgang til det webbaserte verktøyet for broen, eller velg **Disabled** (Deaktivert) for å blokkere trådløs tilgang til verktøyet.

Backup and Restore (Sikkerhetskopier og gjenopprett)

Backup (Sikkerhetskopier) Hvis du vil ta en sikkerhetskopi av konfigurasjonsfilen for broen, klikker du på **Backup Configurations** (Ta sikkerhetskopi av konfigurasjoner). Følg deretter instruksjonene på skjermen.

Restore (Gjenopprett) Klikk på **Browse** (Bla gjennom), og velg konfigurasjonsfilen. Klikk deretter på **Restore Configurations** (Gjenopprett konfigurasjoner).

System Reboot (Systemomstart)

Reboot (Omstart) Hvis du vil foreta omstart eller starte broen på nytt, klikker du på **Start to Reboot** (Start omstart).

Klikk på **Save Settings** (Lagre innstillinger) for å ta i bruk endringene, eller klikk på **Cancel Changes** (Forkast endringer) for å forkaste endringene.

Administration (Administrasjon) > Factory Defaults (Fabrikkstandarder)

Bruk dette skjermbildet til å gjenopprette brokonfigurasjonen til fabrikkstandardene.

Factory Defaults (Fabrikkstandarder)

Restore All Settings (Gjenopprett alle innstillinger) Hvis du vil tilbakestille broinnstillingene til fabrikkstandardene, klikker du på **Restore All Settings** (Gjenopprett alle innstillinger). Alle innstillinger du har lagret, går tapt når du gjenoppretter fabrikkinnstillingene.



Administration (Administrasjon) > Upgrade Firmware (Oppgrader fastvare)

Bruk dette skjermbildet til å oppgradere fastvaren for broen. Ikke oppgrader fastvaren med mindre du har problemer med broen eller den nye fastvaren har en funksjon du vil bruke.



Før du oppgraderer fastvaren, laster du ned filen med fastvareoppgraderingen for broen fra webområdet til Linksys, **www.linksys.com/support**.

Upgrade Firmware (Oppgrader fastvare)

Please select a file to upgrade the firmware (Velg en fil for å oppgradere fastvaren) Klikk på **Browse** (Bla gjennom), og velg filen med fastvareoppgraderingen. Klikk deretter på **Start to Upgrade** (Start oppgradering), og følg instruksjonene på skjermen.

Status > Bridge (Bro)

Gjeldende statusinformasjon for broen vises.



Bridge Information (Broinformasjon)

Firmware Version (Fastvareinformasjon) Gjeldende fastvare for broen vises.

Local Network (Lokalt nettverk)

Local MAC Address (Lokal MAC-adresse) MAC-adressen for broen, slik den er i det lokale Ethernet-nettverket, vises.

IP Address (IP-adresse) IP-adressen for broen, slik den er i det lokale Ethernet-nettverket, vises.

Subnet Mask (Delnettmaske) Delnettmasken som er konfigurert for det lokale nettverket, vises.

Status > Wireless (Trådløst)

Informasjon om det trådløse nettverket vises.



Wireless (Trådløst)

Link Status (Koblingsstatus) Statusen for tilkoblingen til det trådløse nettverket vises.

MAC Address (MAC-adresse) MAC-adressen for broen, slik den er i det lokale trådløse nettverket, vises.

Network Name (SSID) (Nettverksnavn (SSID)) Navnet på det trådløse nettverket eller SSIDen vises.

BSSID Den trådløse MAC-adressen for den tilkoblede trådløse ruteren (eller tilgangspunktet) vises.

Radio Band (Radiobånd) Radiobåndet for det trådløse nettverket vises.

Channel Width (Kanalbredde) Kanalbredden som brukes i det trådløse nettverket, vises i MHz.

Wide Channel (Bred kanal) Avhengig av kanalinnstillingene for nettverksruteren, vises den brede kanalen. Hvis du valgte Wide - 40MHz Channel (Bred - 40 MHz-kanal) som ruterinnstilling for radiobånd eller kanalbredde, vil dette være den primære Wireless-N-kanalen.

Standard Channel (Standardkanal) Innstillingen for standardkanal vises. Hvis du valgte Wide - 40MHz Channel (Bred - 40 MHz-kanal) som ruterinnstilling for radiobånd eller kanalbredde, vil standardkanalen være en sekundær kanal for Wireless-N.

Bit Rate (Bithastighet) Dataoverføringshastigheten vises.

Signal Signalstyrken i prosent vises. 100% er den sterkeste signalstyrken som er mulig, og 0% er den svakeste styrken som er mulig.

Security (Sikkerhet) Sikkerhetsmetoden for det trådløse nettverket vises.

Feilsøking

WES610N/WET610N

Datamaskinen eller en annen kablet Ethernet-enhet kan ikke kommunisere med den trådløse ruteren.

1. Åpne det webbaserte verktøyet for broen.
2. I skjermbildet *Basic Wireless Settings* (Grunnleggende trådløsinnstillinger) kontrollerer du at nettverksnavnet (SSIDen) samsvarer med navnet på det trådløse nettverket.
3. Kontroller at sikkerhetsinnstillingene (WPA, WPA2 eller WEP) samsvarer med sikkerhetsinnstillingene for det trådløse nettverket.

Broens IP-adresse må endres.

Hvis broen er koblet til et nettverk via en DHCP-server (vanligvis nettverksruteren), vil broen hente IP-adressen fra DHCP-serveren. Hvis det ikke finnes noen DHCP-server, vil broen bruke standard statisk IP-adresse, som er **169.254.1.250**.

Hvis du vil at broen alltid skal bruke en statisk IP-adresse, følger du disse instruksjonene:

1. Åpne det webbaserte verktøyet for broen.
2. Klikk på kategorien **Network Setup** (Nettverkskonfigurasjon).
3. Velg *Static IP* (Statisk IP) på hurtigmenyen **Network Connection Type** (Nettverkstilkoblingstype).
4. Fyll ut feltene *Static IP Address* (Statisk IP-adresse), *Subnet Mask* (Delnettmaske) og *Default Gateway* (Standardgateway).
5. Klikk på **Save Settings** (Lagre innstillinger).

Den broaktiverte datamaskinen eller en annen kablet Ethernet-enhet vil ikke kommunisere med en annen trådløsaktivert enhet (for eksempel en datamaskin eller skriver).

Kontroller følgende:

- Kontroller at den trådløsaktiverte enheten er i det samme trådløse nettverket som datamaskinen eller en annen kablet Ethernet-enhet som er koblet til broen.
- Kontroller at samme nettverksnavn (SSID) brukes for alle enheter i det trådløse nettverket.
- Kontroller at alle enheter er i samme IP-nettverk og bruker kompatible IP-adresser.

Det webbaserte verktøyet godtar ikke passordet ditt.

Kontroller følgende:

- Passordet skiller mellom store og små bokstaver. Pass på at du bruker riktig bokstavtype når du angir passordet.
- Hvis du glemmer passordet, kan du tilbakestille broen til fabrikkstandardene.

 Trykk på og hold inne knappen **Reset** (Tilbakestill) på broen i ca. fem sekunder. Passordet vil bli tilbakestilt til fabrikkstandarden, som er **admin**. Alle andre broinnstillinger vil også bli tilbakestilt til fabrikkstandardene. (Du åpner det webbaserte verktøyet ved å angi **admin** i feltet *Password* (Passord).)

Når du har gjort endringene i det webbaserte verktøyet, vises ikke de nye innstillingene på skjermen.

Klikk på **Oppdater** i webleseren. Følg disse instruksjonene hvis de nye innstillingene ikke vises:

1. Koble strømadapteren fra broen.
2. Vent fem sekunder, og koble deretter strømadapteren til broen igjen.
3. Klikk på **Oppdater** i webleseren.

WEB
Hvis spørsmålene dine ikke ble besvart her, kan du gå til webområdet for Linksys på **Linksys.com/support**

Spesifikasjoner

WES610N

Modell	WES610N
Standarder	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Lamper	Strøm, Ethernet, Wi-Fi Protected Setup™, Trådløst, individuell Ethernet-kobling og aktivitet
Porter	Ethernet (4), strøm
Knapper	Reset (Tilbakestill), Wi-Fi Protected Setup
Kabeltype	CAT5e
Antenner	3 (interne)
Antennetilkoblingstype	I/T
Avtakbar (ja/nei)	Nei
Moduleringer	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF-effekt (EIRP) i dBm	802.11a: 15 dBm (vanlig) ved 54 Mbps 802.11b: 19 dBm (vanlig) ved 11 Mbps 802.11g: 16 dBm (vanlig) ved 54 Mbps 802.11n (2,4 GHz): 18 dBm (vanlig) ved MCS15 802.11n (5 GHz): 16 dBm (vanlig) ved MCS15
Mottakssensitivitet	802.11a: -72 dBm (vanlig) ved 54 Mbps 802.11b: -85 dBm (vanlig) ved 11 Mbps 802.11g: -73 dBm (vanlig) ved 54 Mbps 802.11n (20 MHz): -75 dBm (vanlig) ved MCS15 802.11n (40 MHz): -69 dBm (vanlig) ved MCS15
Antenneforsterkning i dBi	1
Trådløs sikkerhet	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Sikkerhetsnøkkelbiter	Opptil 128-biters kryptering

Omgivelser

Mål	177 cm x 128 cm x 68 cm
Vekt	295 g
Sertifisering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Strøm	12 V, 1 A
Driftstemperatur	0 til 40 °C
Oppbevaringstemperatur	-20 til 60 °C
Luftfuktighet for drift	10–85 % ikke-kondenserende
Luftfuktighet for oppbevaring	5–90 % ikke-kondenserende

Spesifikasjonene kan endres uten varsel.

WET610N

Modell	WET610N
Standarder	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Lamper	Strøm, Ethernet, Wi-Fi Protected Setup™, Trådløst
Porter	Ethernet, strøm
Knapper	Reset (Tilbakestill), Wi-Fi Protected Setup
Kabeltype	CAT5e
Antenner	3 (interne)
Antennetilkoblingstype	I/T
Avtakbar (ja/nei)	Nei
Moduleringer	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF-effekt (EIRP) i dBm	802.11a: 15 dBm (vanlig) ved 54 Mbps 802.11b: 18 dBm (vanlig) ved 11 Mbps 802.11g: 16 dBm (vanlig) ved 54 Mbps 802.11n: 12 dBm (vanlig) ved 130 Mbps (HT20), 270 Mbps (HT40)
Mottakssensitivitet	802.11a: -72 dBm (vanlig) ved 54 Mbps 802.11b: -85 dBm (vanlig) ved 11 Mbps 802.11g: -73 dBm (vanlig) ved 54 Mbps 802.11n: -70 dBm (vanlig) ved MCS15 / 2,4 GHz, -69 dBm (vanlig) ved MCS15 / 5,0 GHz
Antenneforsterkning i dBi	1
Trådløs sikkerhet	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Sikkerhetsnøkkelbiter	Opptil 128-biters kryptering

Omgivelser

Mål	145 cm x 106 cm x 52 cm
Vekt	159 g
Sertifisering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Strøm	12 V, 1 A
Driftstemperatur	0 til 40 °C
Oppbevaringstemperatur	-20 til 60 °C
Luftfuktighet for drift	10–85 % ikke-kondenserende
Luftfuktighet for oppbevaring	5–90 % ikke-kondenserende

Spesifikasjonene kan endres uten varsel.

Linksys.com/support

Cisco, Cisco-logoen og Linksys er varemerker eller registrerte varemerker for Cisco og/eller selskapets tilknyttede selskaper i USA og andre land.
Du kan finne en oversikt over Ciscos varemerker på www.cisco.com/go/trademarks. Alle andre varemerker nevnt i dette dokumentet, tilhører de respektive eierne.

© 2011 Cisco og/eller tilknyttede selskaper. Med enerett.

3425-01249



Podręcznik użytkownika

Linksys WET610N/WES610N | Most Dual-Band N Entertainment Bridge

Zawartość

Opis produktu

Panel diod LED 2
Panel portów 3

Zabezpieczenia sieci bezprzewodowej — lista kontrolna

Zmień domyślną nazwę sieci bezprzewodowej (SSID) 4
Zmień domyślne hasło 4
Włącz filtrowanie adresów MAC 4
Włącz szyfrowanie 4

Ogólne wytyczne dotyczące zabezpieczania sieci 4
Dodatkowe wskazówki dotyczące bezpieczeństwa 5

Konfiguracja zaawansowana

Dostęp do narzędzia WWW 6
Setup > Basic Setup (Konfiguracja > Konfiguracja podstawowa) . . . 7
Język 7
Konfiguracja sieci 7
Wireless > Basic Wireless Settings (Połączenie bezprzewodowe > Podstawowe ustawienia bezprzewodowe) 7
Podstawowe ustawienia sieci bezprzewodowej 8
Zabezpieczenia sieci bezprzewodowej 8
Chroniona konfiguracja sieci Wi-Fi 9
Wireless — Wireless Network Site Survey (Połączenie bezprzewodowe — Badanie lokalizacji sieci bezprzewodowej) 10
Wireless Network Site Survey (Badanie lokalizacji sieci bezprzewodowej) 10
Wireless > WMM® (Sieć bezprzewodowa > WMM®) 11
WMM 12
Wireless > Advanced Wireless Settings (Połączenie bezprzewodowe > Zaawansowane ustawienia bezprzewodowe) 13
Zaawansowane ustawienia bezprzewodowe 14
Administration > Management (Administracja > Zarządzanie) . . . 14
Management (Zarządzanie) 15
Administration > Factory Defaults (Administracja > Domyślne ustawienia fabryczne) 15
Domyślne ustawienia fabryczne 15
Administration > Upgrade Firmware (Administracja > Uaktualnienie oprogramowania sprzętowego) 15
Uaktualnienie oprogramowania sprzętowego 16
Status > Bridge (Stan > Most) 16
Bridge Information (Informacje o moście) 16
Sieć lokalna 16
Status > Wireless (Stan > Połączenie bezprzewodowe) 16
Wireless (Połączenie bezprzewodowe) 16

Rozwiązywanie problemów

WES610N/WET610N 17

Dane techniczne

WES610N 18
WET610N 19

Opis produktu

Dziękujemy za wybranie mostu Linksys Dual-Band N Entertainment Bridge. Most umożliwia podłączenie dowolnego przewodowego urządzenia Ethernet do sieci bezprzewodowej. Most wykorzystuje technologię Dual-Band Wireless-N, dzięki czemu jest zgodny z dowolnym routerem lub punktem dostępowym Wireless-N, -G, -A lub -B. Jeśli produkt jest instalowany po raz pierwszy, wykonaj kroki w folderze CD. Aby skonfigurować ustawienia zaawansowane, skorzystaj z wygodnego narzędzia WWW.

Panel diod LED



WES610N WET610N

Połączenie bezprzewodowe (kolor niebieski) Dioda LED połączenia bezprzewodowego zapala się, gdy istnieje połączenie bezprzewodowe. Dioda LED miga, gdy most przesyła lub odbiera dane za pośrednictwem sieci bezprzewodowej.

Przycisk Wi-Fi Protected Setup Jeśli router obsługuję funkcję Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi) i używa zabezpieczeń WPA lub WPA2, można użyć tej funkcji w celu automatycznego połączenia mostu. Aby użyć funkcji Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi), zapoznaj się z częścią „Wireless > Basic Wireless Settings (Połączenie bezprzewodowe > Podstawowe ustawienia bezprzewodowe)" na str. 7.

Dioda LED Wi-Fi Protected Setup (kolor niebieski/pomarańczowy) Ta dioda LED miga na niebiesko przez dwie minuty w trakcie działania funkcji Wi-Fi Protected Setup. Zapala się na niebiesko, gdy włączone są zabezpieczenia sieci bezprzewodowej. Jeśli podczas działania procesu Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi) wystąpi błąd, dioda LED świeci na pomarańczowo. Upewnij się, że router sieciowy obsługuje funkcję Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi). Zaczekaj aż dioda LED przestanie świecić i spróbuj ponownie.

Połączenie Ethernet (kolor niebieski) Dioda LED połączenia Ethernet zapala się, gdy istnieje połączenie przewodowe. Dioda LED miga, gdy most przesyła lub odbiera dane przez porty Ethernet.

Zasilanie (kolor niebieski) Dioda LED zasilania zapala się, gdy zostanie włączone zasilanie mostu.

Panel portów



WES610N WET610N

Ethernet Przy użyciu portów Ethernet można podłączyć most do komputera lub innego urządzenia sieciowego Ethernet. Model WES610N ma cztery porty, a model WET610N — jeden port.

Reset Istnieją dwa sposoby na przywracanie domyślnych fabrycznych ustawień mostu. Można nacisnąć przycisk Reset i przytrzymać go przez mniej więcej pięć sekund lub przywrócić ustawienia domyślne z poziomu ekranu Administration > Factory Defaults (Administracja > Domyślne ustawienia fabryczne) narzędzia WWW mostu. Model WES610N ma przycisk Reset na spodzie urządzenia, a model WET610N — na tylnym panelu portów.

Zasilanie Port zasilania służy do podłączenia do mostu dostarczonego zasilacza.

Zabezpieczenia sieci bezprzewodowej — lista kontrolna

Sieci bezprzewodowe można instalować w prosty i wygodny sposób, więc liczba gospodarstw domowych z szerokopasmowym dostępem do Internetu, w których są one instalowane, gwałtownie rośnie. Ponieważ sieci bezprzewodowe działają na zasadzie przesyłania informacji za pomocą fali radiowych, mogą one być bardziej narażone na włamania niż sieci tradycyjne. Podobnie jak ma to miejsce w przypadku telefonów komórkowych czy bezprzewodowych, sygnały z sieci bezprzewodowych można przechwytywać. Ponieważ nie można fizycznie uniemożliwić innym osobom łączenia się z siecią bezprzewodową, należy podjąć dodatkowe kroki w celu jej zabezpieczenia.

Zmień domyślną nazwę sieci bezprzewodowej (SSID)

Bezprzewodowe urządzenia mają fabrycznie ustawianą, domyślną nazwę sieci bezprzewodowej, która określana jest także mianem identyfikatora SSID (Service Set Identifier). Jest to nazwa sieci bezprzewodowej, która może składać się z maksymalnie 32 znaków. Domyślną nazwą sieci bezprzewodowej w urządzeniach firmy Linksys jest **linksys**. Nazwę sieci bezprzewodowej należy zmienić na coś unikatowego, co wyróżni sieć spośród innych sieci bezprzewodowych, które mogą występować w okolicy. Nie powinny być jednak wykorzystywane dane osobowe (np. numer PESEL), ponieważ informacje te mogą być dostępne dla każdego wyszukującego sieci bezprzewodowe.

Zmień domyślne hasło

W przypadku produktów bezprzewodowych, takich jak punkty dostępowe i routery, przy próbie zmiany ustawień pojawia się prośba o podanie hasła. Urządzenia tego typu mają fabrycznie ustawiane hasło domyślne. Domyślne hasło firmy Linksys to **admin**. Hakerzy znają te domyślne hasła i mogą próbować wykorzystać je w celu uzyskania dostępu do urządzenia i zmiany ustawień sieciowych. Aby uniemożliwić wprowadzanie nieautoryzowanych zmian, należy zmienić hasło tak, aby trudno było je odgadnąć.

Włącz filtrowanie adresów MAC

Routery firmy Linksys dają możliwość filtrowania adresów Media Access Control (MAC). Adres MAC to unikatowa seria liczb oraz liter przypisywana do każdego urządzenia sieciowego. Po włączeniu funkcji filtrowania adresów MAC bezprzewodowy dostęp do sieci uzyskują wyłącznie urządzenia o wskazanych adresach MAC. Można na przykład podać adresy MAC wszystkich komputerów domowych, aby tylko one mogły mieć dostęp do sieci bezprzewodowej.

Włącz szyfrowanie

Szyfrowanie zabezpiecza dane przesyłane w sieci bezprzewodowej. Standardy szyfrowania WPA/WPA2 (Wi-Fi Protected Access) oraz WEP (Wired Equivalent Privacy) zapewniają różne stopnie ochrony dla sieci bezprzewodowych.

Sieć zabezpieczona szyfrowaniem WPA/WPA2 jest bezpieczniejsza od sieci z szyfrowaniem WEP, ponieważ szyfrowanie WPA/WPA2 wykorzystuje dynamiczne szyfrowanie kluczem. Aby chronić informacje przesyłane falami radiowymi, należy włączyć najwyższy z dostępnych poziomów zabezpieczeń obsługiwanych przez wyposażenie sieciowe.

WEP to starszy standard szyfrowania, który może być jedyną dostępną opcją w starszych urządzeniach, które nie obsługują szyfrowania WPA.

Ogólne wytyczne dotyczące zabezpieczania sieci

Zabezpieczanie sieci bezprzewodowej nie ma sensu, jeśli sieć bazowa nie jest bezpieczna.

- Wszystkie komputery powinny być chronione hasłami, podobnie jak najważniejsze pliki.
- Hasła powinny być regularnie zmieniane.
- Należy zainstalować oprogramowanie antywirusowe oraz zapory ogniowe.
- Należy wyłączyć funkcję wymiany plików (peer-to-peer). Niektóre aplikacje mogą uaktywniać funkcję wymiany plików bez zgody oraz wiedzy użytkownika.

Dodatkowe wskazówki dotyczące bezpieczeństwa

- Routery bezprzewodowe, punkty dostępowe oraz bramki powinny znajdować się z dala od ścian zewnętrznych i okien.
- Routery bezprzewodowe, punkty dostępowe oraz bramki należy wyłączać, gdy nie są używane (w nocy, w czasie urlopów).
- Należy używać trudnych do odgadnięcia haseł, składających się z co najmniej ośmiu znaków. Należy w nich łączyć litery oraz cyfry, aby uniknąć używania wyrazów, które można znaleźć w słowniku.

Konfiguracja zaawansowana

Po skonfigurowaniu mostu poprzez wykonanie kroków w folderze CD będzie on gotowy do użytku. Aby jednak zmienić ustawienia zaawansowane, należy skorzystać z narzędzia WWW do konfiguracji mostu. W tym rozdziale opisano poszczególne strony narzędzia oraz kluczowe funkcje każdej z nich. Dostęp do narzędzia można uzyskać za pomocą przeglądarki internetowej komputera podłączonego do mostu.

Narzędzie WWW zawiera następujące podstawowe karty: Setup Konfiguracja), Wireless (Połączenie bezprzewodowe), Administration (Administracja) oraz Status (Stan). Dodatkowe karty są dostępne po kliknięciu jednej z głównych kart.

Dostęp do narzędzia WWW

Dostęp do narzędzia WWW można uzyskać za pomocą przeglądarki internetowej.

Jeśli most jest podłączony do sieci z serwerem DHCP (zazwyczaj jest nim router), to uzyskuje swój adres IP z tego serwera. W przypadku braku serwera DHCP most używa domyślnego, statycznego adresu IP **169.254.1.250**. (Jeśli za pomocą narzędzia WWW ustawiono trwały statyczny adres IP mostu, należy wprowadzić ten statyczny adres IP).

UWAGA
Jeśli nie znasz adresu IP mostu, możesz go znaleźć w tabeli klientów DHCP routera. (Patrz dokumentacja routera).

Jeśli nie możesz znaleźć adresu IP mostu, możesz zresetować most. W tym celu naciśnij przycisk **Reset** mostu przy użyciu wyprostowanego spinacza do papieru i przytrzymaj go przez około pięć sekund. Spowoduje to przywrócenie domyślnych ustawień fabrycznych mostu. Most zażąda adresu IP od serwera DHCP (zazwyczaj routera sieciowego). Jeśli serwer DHCP nie zostanie znaleziony, most będzie używać domyślnego statycznego adresu IP **169.254.1.250** do momentu wykrycia serwera DHCP i przypisania dynamicznego adresu IP.

Jeśli most nie jest połączony z routerem i używa domyślnych ustawień fabrycznych, podłącz komputer do mostu przy użyciu połączenia Ethernet w celu uzyskania dostępu do narzędzia WWW. Połączenie Ethernet należy skonfigurować na komputerze przy użyciu statycznego adresu IP i maski podsieci.

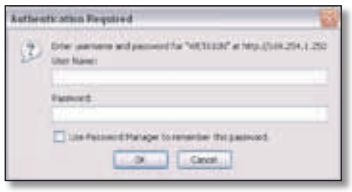
Adres IP karty sieciowej Ethernet należy ustawić na określony adres IP.

1. W polu *Adres IP* wprowadź **169.254.x.y** (znak x należy zastąpić liczbą z przedziału od 1 do 254, a znak y — liczbą z przedziału od 0 do 255).
2. W polu *Maska podsieci* wprowadź **255.255.0.0**.

UWAGA
Procedura przypisywania statycznego adresu IP do karty sieciowej Ethernet w komputerze różni się w zależności od używanego systemu operacyjnego. Instrukcje można znaleźć w dokumentacji pomocy określonego systemu operacyjnego.

Po przypisaniu statycznego adresu IP do karty sieciowej Ethernet uruchom przeglądarkę internetową i wprowadź adres IP mostu (ustawienie domyślne to **169.254.1.250**) w polu *Adres*. Naciśnij klawisz **Enter**

Zostanie wyświetlony ekran żądania hasła (podobny ekran zostanie wyświetlony w przypadku używania innego systemu operacyjnego niż Windows XP). Pole *Nazwa użytkownika* pozostaw puste. Wprowadź hasło utworzone podczas działania Kreatora instalacji. Jeśli nowe hasło nie zostało utworzone, użyj domyślnego hasła **admin**. Nowe hasło można ustawić na ekranie *Administration* > *Management* (Administracja > Zarządzanie). Kliknij przycisk **OK**, aby kontynuować.



UWAGA
Jeśli ekran żądania hasła nie zostanie wyświetlony, odczekaj dwie minuty i spróbuj ponownie.

Setup > Basic Setup (Konfiguracja > Konfiguracja podstawowa)

Jako pierwszy jest wyświetlany ekran *Basic Setup* (Konfiguracja podstawowa). Umożliwia on zmianę języka narzędzia WWW oraz zmianę ustawień mostu dotyczących przewodowej sieci Ethernet.





Język

Language (Język) Opcja pozwalająca ustawić język używany w narzędziu WWW. Wybierz odpowiedni język z menu rozwijanego.

Konfiguracja sieci

Ta sekcja określa, czy most pobiera adres IP automatycznie z serwera DHCP, np. routera sieciowego (Automatic Configuration - DHCP (Konfiguracja automatyczna - DHCP)), czy też jest on ustawiany ręcznie (Static IP (Statyczny adres IP)).

Bridge IP (Adres IP mostu) Jeśli w sieci jest serwer DHCP, np. router sieciowy, który przypisuje adresy IP urządzeniom sieciowym, pozostaw ustawienie domyślne **Automatic Configuration - DHCP** (Automatyczna konfiguracja - DHCP). Most zażąda adresu IP od serwera DHCP (zazwyczaj routera sieciowego). Jeśli serwer DHCP nie zostanie znaleziony, most będzie używać domyślnego statycznego adresu IP **169.254.1.250** do momentu wykrycia serwera DHCP i przypisania dynamicznego adresu IP.

Aby ustawić stały, statyczny adres IP dla mostu, wybierz opcję **Static IP** (Statyczny adres IP).

Po wybraniu opcji Static IP należy wypełnić następujące pola:

- **Static IP Address** (Statyczny adres IP) Wprowadź niepowtarzalny adres IP, który będzie służył do uzyskiwania dostępu do narzędzia WWW.
- **Subnet Mask** (Maska podsieci) Wprowadź maskę podsieci dla sieci przewodowej.
- **Default Gateway** (Brama domyślna) Wprowadź adres IP domyślnej bramy swojej sieci (w większości przypadków jest nią router).

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Wireless > Basic Wireless Settings (Połączenie bezprzewodowe > Podstawowe ustawienia bezprzewodowe)

Ekran *Basic Wireless Settings* (Podstawowe ustawienia sieci bezprzewodowej) pozwala skonfigurować podstawowe ustawienia sieci bezprzewodowej i zabezpieczeń mostu.

Ustawienia mostu można skonfigurować na dwa sposoby: ręcznie lub poprzez funkcję Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi). Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi) to funkcja, która ułatwia dokonywanie ustawień sieci bezprzewodowych. Jeśli router obsługuję funkcję Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi) i używa zabezpieczeń WPA lub WPA2, można użyć tej funkcji w celu automatycznego połączenia mostu.

Configuration View (Widok konfiguracji) Aby skonfigurować sieć bezprzewodową samodzielnie, wybierz opcję **Manual** (Ręcznie). Patrz sekcja **Podstawowe ustawienia sieci bezprzewodowej**, **str. 8**. Aby zastosować chronioną konfigurację sieci Wi-Fi, wybierz opcję **Wi-Fi Protected Setup** (Chroniona konfiguracja sieci Wi-Fi). Patrz sekcja **Chroniona konfiguracja sieci Wi-Fi**, **str. 9**.

Podstawowe ustawienia sieci bezprzewodowej



Network Name (SSID) (Nazwa sieci (SSID)) SSID to nazwa sieci wspólna dla wszystkich punktów w sieci bezprzewodowej. Nazwa SSID musi być jednakowa dla wszystkich urządzeń w sieci bezprzewodowej. W nazwie tej jest uwzględniana wielkość liter, a jej długość nie może przekroczyć 32 znaków (może składać się z dowolnych znaków klawiaturowych). Ustawienie to musi odpowiadać temu, który wprowadzono w routerze bezprzewodowym lub punkcie dostępowym. Aby zwiększyć bezpieczeństwo, warto zmienić domyślną nazwę SSID (**linksys**) na inną, niepowtarzalną nazwę.

Zabezpieczenia sieci bezprzewodowej

Most obsługuje następujące opcje zabezpieczeń sieci bezprzewodowej: WPA Personal, WPA2 Personal i WEP. WPA (Wi-Fi Protected Access) i WPA2 to zabezpieczenia o większej sile niż WEP (Wired Equivalent Privacy). Więcej informacji o zabezpieczeniach sieci bezprzewodowej można znaleźć w sekcji „Zabezpieczenia sieci bezprzewodowej — lista kontrolna", str. 4.

Security Mode (Tryb zabezpieczenia)

Wybierz metodę zabezpieczenia sieci bezprzewodowej. Jeśli nie chcesz korzystać z zabezpieczeń sieci bezprzewodowej, zachowaj ustawienie domyślne, **Disabled** (Wył.).

UWAGA
Każde urządzenie w sieci bezprzewodowej MUSI korzystać z tej samej metody zabezpieczeń oraz hasła/klucza. W przeciwnym wypadku urządzenia bezprzewodowe nie będą mogły komunikować się ze sobą.

WPA Personal

WPA to standard zabezpieczeń silniejszy niż szyfrowanie WEP.



Encryption (Szyfrowanie) Standard WPA obsługuje metodę szyfrowania TKIP z dynamicznymi kluczami szyfrowania.

Passphrase (Hasło) Wprowadź klucz współużytkowany przez most i router bezprzewodowy lub punkt dostępowy. Klucz musi mieć od 8 do 63 znaków.

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

WPA2 Personal

WPA2 to bardziej zaawansowana i bezpieczniejsza wersja standardu WPA.



Encryption (Szyfrowanie) Tryb WPA2 obsługuje dwie metody szyfrowania, TKIP oraz AES, wykorzystujące dynamiczne szyfrowanie kluczem. Wybierz metodę szyfrowania **AES** albo **TKIP lub AES**. Ustawienie domyślne to **AES**.

Passphrase (Hasło) Wprowadź klucz współużytkowany przez most i router bezprzewodowy lub punkt dostępowy. Klucz musi mieć od 8 do 63 znaków.

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

WEP

WEP to podstawowa metoda szyfrowania, która nie zapewnia tak wysokiego poziomu bezpieczeństwa jak WPA czy WPA2.



Encryption (Szyfrowanie) Wybierz poziom szyfrowania WEP, **40/64 bits (10 hex digits)** (40/64 bity (10 cyfr szesnastkowych)) lub **104/128 bits (26 hex digits)** (104/128 bitów (26 cyfr szesnastkowych). Poziom domyślny to **40/64 bits (10 hex digits)** (40/64 bity (10 cyfr szesnastkowych)).

Key 1 (Klucz 1) Wprowadź klucz WEP swojej sieci.

Tx Key (Klucz Tx) **Key 1** to klucz transmisji używany przez most.

Authentication (Uwierzytelnianie) Ustawienie domyślne to **Auto** (Automatycznie), co pozwala na stosowanie uwierzytelniania Open System (otwartego) lub Shared Key (kluczem wspólnym). Wybierz opcję **Open** (Otwarte), aby użyć uwierzytelniania otwartego (Open System). W tym przypadku nadawca i odbiorca nie używają klucza WEP do uwierzytelniania. Wybierz opcję **Shared** (Klucz wspólny), aby użyć uwierzytelniania kluczem wspólnym. W tym przypadku nadawca i odbiorca używają klucza WEP do uwierzytelniania.

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Chroniona konfiguracja sieci Wi-Fi

Istnieją dwie możliwe metody. Zastosuj metodę odpowiednią dla używanego routera.





Metoda nr 1

Metodę tę stosuje się w przypadku routera z przyciskiem Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi).

1. Kliknij lub naciśnij przycisk **Wi-Fi Protected Setup** (Chroniona konfiguracja sieci Wi-Fi) znajdujący się na routerze.
2. W ciągu dwóch minut kliknij przycisk **Wi-Fi Protected Setup** (Chroniona konfiguracja sieci Wi-Fi) na ekranie mostu *Wi-Fi Protected Setup* (Chroniona konfiguracja sieci Wi-Fi).
3. Po skonfigurowaniu mostu kliknij przycisk **Close** (Zamknij).

Na ekranie *Wi-Fi Protected Setup* (Chroniona konfiguracja sieci Wi-Fi) wyświetlane są informacje o stanie łącza, nazwie sieci (SSID) i metodzie zabezpieczeń.

Metoda nr 2

Metodę tę stosuje się w przypadku, gdy router żądania podania numeru PIN mostu.

1. Na ekranie **routera** *Wi-Fi Protected Setup* (Chroniona konfiguracja sieci Wi-Fi) wprowadź numer PIN z ekranu **mostu** *Wi-Fi Protected Setup* (Chroniona konfiguracja sieci Wi-Fi). Następnie naciśnij przycisk **Zarejestruj** lub inny odpowiedni przycisk (Jest on umieszczony również na etykiecie na spodzie mostu).
2. Na ekranie **mostu** *Wi-Fi Protected Setup* (Chroniona konfiguracja sieci Wi-Fi) kliknij przycisk **OK**.
3. Po skonfigurowaniu mostu kliknij przycisk **Close** (Zamknij).

Na ekranie *Wi-Fi Protected Setup* (Chroniona konfiguracja sieci Wi-Fi) wyświetlane są informacje o stanie łącza, nazwie sieci (SSID) i metodzie zabezpieczeń.

Wireless — Wireless Network Site Survey (Połączenie bezprzewodowe — Badanie lokalizacji sieci bezprzewodowej)

Kliknij kartę **Wireless Network Site Survey** (Badanie lokalizacji sieci bezprzewodowej), aby rozpocząć badanie lokalizacji. Na ekranie *Wireless Network Site Survey* (Badanie lokalizacji sieci bezprzewodowej) wyświetlana jest lista sieci bezprzewodowych wykrytych przez most.



Wireless Network Site Survey (Badanie lokalizacji sieci bezprzewodowej)

Number of Wireless Networks (Liczba sieci bezprzewodowych) Wyświetlana jest liczba sieci bezprzewodowych wykrytych przez most.

Select (Wybierz) Aby połączyć się z siecią bezprzewodową, kliknij opcję **Select** (Wybierz). Następnie kliknij opcję **Connect** (Połącz).

Wireless Network Name (Nazwa sieci bezprzewodowej) Wyświetlana jest nazwa lub identyfikator SSID sieci bezprzewodowej.

GHz Wyświetlane jest pasmo radiowe sieci bezprzewodowej.

Signal (Sygnał) Wyświetlana jest procentowa siła sygnału. 100% oznacza najmocniejszą możliwą siłę sygnału, natomiast 0% oznacza najsłabszy możliwy sygnał.

Security (Zabezpieczenia) Jeśli sieć obsługuje funkcję Wi-Fi Protected Setup (Chroniona konfiguracja sieci Wi-Fi), wyświetlana jest ikona Wi-Fi Protected Setup . Wyświetlane są informacje o metodzie zabezpieczeń używanej w sieci bezprzewodowej.

Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować dane wyświetlane na ekranie.

Po wybraniu sieci kliknij opcję **Connect** (Połącz). Zostanie wyświetlony nowy ekran. Postępuj zgodnie z instrukcjami dla metody zabezpieczeń używanej w sieci.

WPA



Network Name (SSID) (Nazwa sieci (SSID)) Nazwa wybranej sieci jest wyświetlana automatycznie.

Security Mode (Tryb zabezpieczeń) Tryb WPA Personal jest wyświetlany automatycznie.

Encryption (Szyfrowanie) Standard WPA obsługuje metodę szyfrowania TKIP z dynamicznymi kluczami szyfrowania.

Passphrase (Hasło) Wprowadź klucz współużytkowany przez most i router bezprzewodowy lub punkt dostępowy. Klucz musi mieć od 8 do 63 znaków.

Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować dane wyświetlane na ekranie.

Po wybraniu ustawień zabezpieczeń kliknij opcję **Connect** (Połącz).

WPA2



Network Name (SSID) (Nazwa sieci (SSID)) Nazwa wybranej sieci jest wyświetlana automatycznie.

Security Mode (Tryb zabezpieczeń) Tryb WPA2 Personal jest wyświetlany automatycznie.

Encryption (Szyfrowanie) Tryb WPA2 obsługuje dwie metody szyfrowania, TKIP oraz AES, wykorzystujące dynamiczne szyfrowanie kluczem. Wybierz metodę szyfrowania **AES** albo **TKIP lub AES**.

Passphrase (Hasło) Wprowadź klucz współużytkowany przez most i router bezprzewodowy lub punkt dostępowy. Klucz musi mieć od 8 do 63 znaków.

Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować dane wyświetlane na ekranie.

Po wybraniu ustawień zabezpieczeń kliknij opcję **Connect** (Połącz).

WEP



Network Name (SSID) (Nazwa sieci (SSID)) Nazwa wybranej sieci jest wyświetlana automatycznie.

Security Mode (Tryb zabezpieczeń) Tryb WEP jest wyświetlany automatycznie.

Encryption (Szyfrowanie) Wybierz poziom szyfrowania WEP, **40/64 bits (10 hex digits)** (40/64 bity (10 cyfr szesnastkowych)) lub **104/128 bits (26 hex digits)** (104/128 bitów (26 cyfr szesnastkowych)).

Key 1 (Klucz 1) Wprowadź klucz WEP swojej sieci.

Tx Key (Klucz Tx) **Key 1** to klucz transmisji używany przez most.

Authentication (Uwierzytelnianie) Ustawienie domyślne to **Auto** (Automatycznie), co pozwala na stosowanie uwierzytelniania Open System (otwartego) lub Shared Key (kluczem wspólnym). Wybierz opcję **Open** (Otwarte), aby użyć uwierzytelniania otwartego (Open System). W tym przypadku nadawca i odbiorca nie używają klucza WEP do uwierzytelniania. Wybierz opcję **Shared** (Klucz wspólny), aby użyć uwierzytelniania kluczem wspólnym. W tym przypadku nadawca i odbiorca używają klucza WEP do uwierzytelniania.

Kliknij przycisk **Refresh** (Odśwież), aby zaktualizować dane wyświetlane na ekranie.

Po wybraniu ustawień zabezpieczeń kliknij opcję **Connect** (Połącz).

Wireless > WMM® (Sieć bezprzewodowa > WMM®)

Konfiguracja ustawień Wireless MultiMedia (WMM). Standard WMM umożliwia określanie priorytetu pakietów na podstawie ich trybu dostępu (typu ruchu): Background (Tło), Best Effort (Najlepsza wartość), Video (Wideo) lub Voice (Głos). Ustawienia te powinny być zmieniane wyłącznie przez doświadczonego administratora, ponieważ nieprawidłowe wartości mogą zmniejszyć wydajność sieci bezprzewodowej.



UWAGA
Ustawienia na ekranie *WMM* są przeznaczone wyłącznie dla doświadczonych użytkowników.

WMM

Tryb dostępu

Czterem dostępnym trybom dostępu można przypisać różne ustawienia. Wybierz tryb, który chcesz skonfigurować: **Background** (Tło), **Best Effort** (Najlepsza wartość), **Video** (Wideo) lub **Voice** (Głos). Postępuj zgodnie z instrukcjami wybranego trybu.

Background (Tło)

Use Aggregation (Użyj agregacji) Ta opcja określa, czy warstwa MAC (Media Access Control) ustawi sesję ADDBA (Add Block Acknowledgement). Ustawieniem domyślnym jest **No** (Nie). Wybierz ustawienie **Yes** (Tak), aby włączyć tę opcję.

Accept Aggregation (Akceptuj agregację) Ta opcja określa, czy warstwa MAC zaakceptuje żądanie ADDBA. Ustawienie domyślne to **Yes** (Tak). Aby wyłączyć to ustawienie, wybierz **No** (Nie).

Max. Number of Packets in Aggregation (Maks. liczba pakietów w agregacji) Ta opcja określa maksymalną liczbę pakietów (ramek podrzędnych) w agregacji. Zakres wynosi od **0** do **7**. Ustawienie domyślne to **7**.

Max. Aggregation Size (Maks. rozmiar agregacji) Ta opcja określa maksymalny rozmiar agregacji (w bajtach). Zakres wynosi od **0** do **16000**. Ustawienie domyślne to **12000**.

Timeout Interval (Interwał limitu czasu) Ta opcja określa limit czasu, w którym agregacja powinna zostać zamknięta przez „warunek zamykający", zanim zostanie zamknięta przez licznik czasu. Zakres wynosi od **0** do **100** ms. Ustawienie domyślne to **3**.

Min. Size of Packet in Aggregation (Min. rozmiar pakietu w agregacji) Ta opcja określa minimalny rozmiar pakietów gromadzonych agregacji (w bajtach). Zakres wynosi od **0** do **1500**. Ustawienie domyślne to **10**.

ADDBA Timeout (Limit czasu ADDBA) Ta opcja określa okres czasu, po upływie którego konfiguracja ADDBA zostaje przerwana, jeśli w jego trakcie nie zachodziły wymiany ramek przez funkcję potwierdzeń blokowych (ACK). Zakres wynosi od **0** do **65535** ms. Ustawienie domyślne to **0**. Powoduje ono wyłączenie limitu czasu.

Aggregation Window Size (Rozmiar okna agregacji) Ta opcja określa maksymalną liczbę pakietów przesyłanych bez uzyskania ACK. Zakres wynosi od **0** do **64**. Ustawienie domyślne to **64**.

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Best Effort (Najlepsza wartość)

Use Aggregation (Użyj agregacji) Ta opcja określa, czy warstwa MAC (Media Access Control) ustawi sesję ADDBA (Add Block Acknowledgement). Ustawienie domyślne to **Yes** (Tak). Aby wyłączyć to ustawienie, wybierz **No** (Nie).

Accept Aggregation (Akceptuj agregację) Ta opcja określa, czy warstwa MAC zaakceptuje żądanie ADDBA. Ustawienie domyślne to **Yes** (Tak). Aby wyłączyć to ustawienie, wybierz **No** (Nie).

Max. Number of Packets in Aggregation (Maks. liczba pakietów w agregacji) Ta opcja określa maksymalną liczbę pakietów (ramek podrzędnych) w agregacji. Zakres wynosi od **0** do **10**. Ustawienie domyślne to **10**.

Max. Aggregation Size (Maks. rozmiar agregacji) Ta opcja określa maksymalny rozmiar agregacji (w bajtach). Zakres wynosi od **0** do **20000**. Ustawienie domyślne to **16000**.

Timeout Interval (Interwał limitu czasu) Ta opcja określa limit czasu, w którym agregacja powinna zostać zamknięta przez „warunek zamykający", zanim zostanie zamknięta przez licznik czasu. Zakres wynosi od **0** do **100** ms. Ustawienie domyślne to **3**.

Min. Size of Packet in Aggregation (Min. rozmiar pakietu w agregacji) Ta opcja określa minimalny rozmiar pakietów gromadzonych agregacji (w bajtach). Zakres wynosi od **0** do **1500**. Ustawienie domyślne to **10**.

ADDBA Timeout (Limit czasu ADDBA) Ta opcja określa okres czasu, po upływie którego konfiguracja ADDBA zostaje przerwana, jeśli w jego trakcie nie zachodziły wymiany ramek przez funkcję potwierdzeń blokowych (ACK). Zakres wynosi od **0** do **65535** ms. Ustawienie domyślne to **0**. Powoduje ono wyłączenie limitu czasu.

Aggregation Window Size (Rozmiar okna agregacji) Ta opcja określa maksymalną liczbę pakietów przesyłanych bez uzyskania ACK. Zakres wynosi od **0** do **64**. Ustawienie domyślne to **64**.

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Video (Filmy)

Use Aggregation (Użyj agregacji) Ta opcja określa, czy warstwa MAC (Media Access Control) ustawi sesję ADDBA (Add Block Acknowledgement). Ustawienie domyślne to **Yes** (Tak). Aby wyłączyć to ustawienie, wybierz **No** (Nie).

Accept Aggregation (Akceptuj agregację) Ta opcja określa, czy warstwa MAC zaakceptuje żądanie ADDBA. Ustawienie domyślne to **Yes** (Tak). Aby wyłączyć to ustawienie, wybierz **No** (Nie).

Max. Number of Packets in Aggregation (Maks. liczba pakietów w agregacji) Ta opcja określa maksymalną liczbę pakietów (ramek podrzędnych) w agregacji. Zakres wynosi od **0** do **7**. Ustawienie domyślne to **7**.

Max. Aggregation Size (Maks. rozmiar agregacji) Ta opcja określa maksymalny rozmiar agregacji (w bajtach). Zakres wynosi od **0** do **16000**. Ustawienie domyślne to **12000**.

Timeout Interval (Interwał limitu czasu) Ta opcja określa limit czasu, w którym agregacja powinna zostać zamknięta przez „warunek zamykający", zanim zostanie zamknięta przez licznik czasu. Zakres wynosi od **0** do **100** ms. Ustawienie domyślne to **3**.

Min. Size of Packet in Aggregation (Min. rozmiar pakietu w agregacji) Ta opcja określa minimalny rozmiar pakietów gromadzonych agregacji (w bajtach). Zakres wynosi od **0** do **1500**. Ustawienie domyślne to **10**.

ADDBA Timeout (Limit czasu ADDBA) Ta opcja określa okres czasu, po upływie którego konfiguracja ADDBA zostaje przerwana, jeśli w jego trakcie nie zachodziły wymiany ramek przez funkcję potwierdzeń blokowych (ACK). Zakres wynosi od **0** do **65535** ms. Ustawienie domyślne to **0**. Powoduje ono wyłączenie limitu czasu.

Aggregation Window Size (Rozmiar okna agregacji) Ta opcja określa maksymalną liczbę pakietów przesyłanych bez uzyskania ACK. Zakres wynosi od **0** do **64**. Ustawienie domyślne to **64**.

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Voice (Głos)

Use Aggregation (Użyj agregacji) Ta opcja określa, czy warstwa MAC (Media Access Control) ustawi sesję ADDBA (Add Block Acknowledgement). Ustawienie domyślne to **Yes** (Tak). Aby wyłączyć to ustawienie, wybierz **No** (Nie).

Accept Aggregation (Akceptuj agregację) Ta opcja określa, czy warstwa MAC zaakceptuje żądanie ADDBA. Ustawienie domyślne to **Yes** (Tak). Aby wyłączyć to ustawienie, wybierz **No** (Nie).

Max. Number of Packets in Aggregation (Maks. liczba pakietów w agregacji) Ta opcja określa maksymalną liczbę pakietów (ramek podrzędnych) w agregacji. Zakres wynosi od **0** do **2**. Ustawienie domyślne to **2**.

Max. Aggregation Size (Maks. rozmiar agregacji) Ta opcja określa maksymalny rozmiar agregacji (w bajtach). Zakres wynosi od **0** do **16000**. Ustawienie domyślne to **10000**.

Timeout Interval (Interwał limitu czasu) Ta opcja określa limit czasu, w którym agregacja powinna zostać zamknięta przez „warunek zamykający", zanim zostanie zamknięta przez licznik czasu. Zakres wynosi od **0** do **100** ms. Ustawienie domyślne to **10**.

Min. Size of Packet in Aggregation (Min. rozmiar pakietu w agregacji) Ta opcja określa minimalny rozmiar pakietów gromadzonych agregacji (w bajtach). Zakres wynosi od **0** do **1500**. Ustawienie domyślne to **10**.

ADDBA Timeout (Limit czasu ADDBA) Ta opcja określa okres czasu, po upływie którego konfiguracja ADDBA zostaje przerwana, jeśli w jego trakcie nie zachodziły wymiany ramek przez funkcję potwierdzeń blokowych (ACK). Zakres wynosi od **0** do **65535** ms. Ustawienie domyślne to **0**. Powoduje ono wyłączenie limitu czasu.

Aggregation Window Size (Rozmiar okna agregacji) Ta opcja określa maksymalną liczbę pakietów przesyłanych bez uzyskania ACK. Zakres wynosi od **0** do **64**. Ustawienie domyślne to **64**.

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Wireless > Advanced Wireless Settings (Połączenie bezprzewodowe > Zaawansowane ustawienia bezprzewodowe)

Konfigurowanie zaawansowanych ustawień funkcji bezprzewodowych mostu. Ustawienia te powinny być zmieniane wyłącznie przez doświadczonego administratora, ponieważ nieprawidłowe wartości mogą zmniejszyć wydajność sieci bezprzewodowej.



UWAGA
Ustawienia na ekranie *Advanced Wireless Settings* (Zaawansowane ustawienia sieci bezprzewodowej) są przeznaczone wyłącznie dla doświadczonych użytkowników.

Zaawansowane ustawienia bezprzewodowe

Use LDPC (Użyj LDPC) Funkcja LDPC (Low-Density Parity-Check Code) umożliwia włączenie lub wyłączenie korekcji błędów w celu zredukowania prawdopodobieństwa utraty danych w zaszumionych kanałach. Algorytm adaptacji szybkości powodował automatyczne wyłączenie kodowania LDPC podczas pracy z dużymi szybkościami PHY (powyżej 162). Aby użyć opcji schematu zaawansowanej korekcji błędów LDCP, zachowaj ustawienie domyślne, **Yes** (Tak). W przeciwnym wypadku wybierz ustawienie **No** (Nie).

ERP Protection Type (Typ ochrony ERP) Ta opcja konfiguruje ochronę pakietów OFDM pomimo obecności stacji 802.11b w sieci bezprzewodowej. Wysyłając pakiety RTS/CTS lub CTS2Self z szybkością 802.11b, most informuje sieć bezprzewodową o przesłaniu pakietów OFDM i chroni te pakiety w sieci bezprzewodowej. Pakiety RTS/CTS i CTS2Self powodują zwiększenie obciążenia, czego wynikiem jest niższa przepustowość.

Opcja RTS/CTS zapewnia lepszy zasięg, ale niższą przepustowość w porównaniu z opcją CTS2Self, ponieważ opcja RTS/CTS obejmuje potwierdzenie z urządzenia odbierającego. Aby użyć opcji RTS/CTS, zachowaj ustawienie domyślne, **RTS/CTS**. Opcja None (Brak) może powodować kolizje między pakietami OFDM i CCK. Aby użyć opcji None (Brak), wybierz ustawienie **None** (Brak). Aby użyć opcji CTS2Self, wybierz ustawienie **CTS2Self**.

11n Protection Type (Typ ochrony 11n) Ta opcja konfiguruje ochronę przed urządzeniami w sieci bezprzewodowej, które nie mają wysokiej przepustowości. W przypadku, gdy router bezprzewodowy (lub punkt dostępowy) wykryje połączenie ze starszym urządzeniem, które nie ma wysokiej przepustowości, będzie sygnalizować wszystkim urządzeniom o wysokiej przepustowości konieczność użycia mechanizmów RTS/CTS lub CTS2Self przed każdą transmisją danych. Ta funkcja obsługuje również wszystkie opcje ochrony standardu 802.11n, w tym MIMO.

Opcja RTS/CTS zapewnia lepszy zasięg, ale niższą przepustowość w porównaniu z opcją CTS2Self, ponieważ opcja RTS/CTS obejmuje potwierdzenie z urządzenia odbierającego. Aby użyć opcji RTS/CTS, zachowaj ustawienie domyślne, **RTS/CTS**. Opcja None (Brak) może powodować kolizje między pakietami z urządzeń o wysokiej przepustowości i pakietami ze starszych urządzeń. Aby użyć opcji None (Brak), wybierz ustawienie **None** (Brak). Aby użyć opcji CTS2Self, wybierz ustawienie **CTS2Self**.

Percentage of maximal transmit power (Procent maksymalnej mocy transmisji) Ta opcja określa procent maksymalnej mocy transmisji w odniesieniu do ograniczeń prawnych danego obszaru działania. Przykładowo, jeśli ograniczenia prawne w danym obszarze działania pozwalają na transmisje z mocą do 20 dB, to ustawienie wartości procentowej 50% umożliwi transmisję z maksymalną mocą 10 dB. Wybierz wartość procentową, której chcesz używać: **12%**, **25%**, **50%** lub **100%**. Ustawienie domyślne to **100%**.

QoS Classification Type (Typ klasyfikacji QoS) Ta opcja ustawia mapowanie 802.1D lub 802.1Q z pola IP DSCP/TOS na priorytety WMM (Background (Tło), Best Effort (Najlepsza wartość), Video (Wideo), Voice (Głos)). Zachowaj ustawienie domyślne, **802.1D**, lub wybierz ustawienie **802.1Q**, które jest używane przez niektóre strumienie IPTV.

Re-establish Ethernet connection when initiating wireless connection (Nawiąż ponownie połączenie Ethernet podczas inicjowania połączenia bezprzewodowego) Aby wywołać wykrywanie DHCP na urządzeniu znajdującym się za mostem, most będzie resetować połączenie Ethernet między mostem a urządzeniem za każdym razem, gdy zostanie nawiązane połączenie bezprzewodowe. Aby wyłączyć to zachowanie, wybierz ustawienie **No** (Nie). W przeciwnym razie zachowaj ustawienie domyślne, **Yes** (Tak).

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Administration > Management (Administracja > Zarządzanie)

Ekran ten umożliwia zarządzanie określonymi funkcjami mostu: dostępem do narzędzia WWW, wykonywaniem kopii zapasowej pliku konfiguracyjnego i ponownym uruchamianiem.



Management (Zarządzanie)

Bridge Access (Dostęp do mostu)

Dostęp do narzędzia WWW można zabezpieczyć przy użyciu hasła.

Bridge Password (Hasło mostu) Wprowadź nowe hasło dostępu do mostu.

Re-enter to confirm (Wprowadź ponownie, aby potwierdzić) Wprowadź hasło ponownie w celu potwierdzenia.

Idle Timeout (Czas bezczynności) Określony przez użytkownika czas bezczynności, po którym następuje wylogowanie. Zakres wynosi od **60** do **3600** s. Ustawienie domyślne to **600**.

Web Access (Dostęp przez Internet)

Access via Wireless (Dostęp przez sieć bezprzewodową) Używając mostu w domenie publicznej i zapewniając gościom dostęp bezprzewodowy, można wyłączyć dostęp bezprzewodowy do narzędzia WWW mostu. Po wyłączeniu tej opcji dostęp do narzędzia WWW będzie możliwy tylko przez połączenie przewodowe. Aby zezwolić na dostęp bezprzewodowy do narzędzia WWW mostu, zachowaj ustawienie domyślne, **Enabled** (Wł.). Aby uniemożliwić dostęp bezprzewodowy do tego narzędzia, wybierz ustawienie **Disabled** (Wył.).

Tworzenie i przywracanie kopii zapasowych

Backup (Kopia zapasowa) Aby utworzyć kopię zapasową pliku konfiguracyjnego mostu, kliknij przycisk **Backup Configurations** (Kopia zapasowa konfiguracji). Następnie wykonuj instrukcje wyświetlane na ekranie.

Restore (Przywracanie) Kliknij przycisk **Browse** (Przeglądaj) i wybierz plik konfiguracyjny. Następnie kliknij przycisk **Restore Configurations** (Przywróć konfigurację)

Ponowne uruchomienie systemu

Reboot (Ponowne uruchamianie) Aby ponownie uruchomić most, kliknij przycisk **Start to Reboot** (Rozpocznij ponowne uruchomienie).

Aby zachować zmiany, kliknij przycisk **Save Settings** (Zapisz ustawienia). W przeciwnym razie kliknij przycisk **Cancel Changes** (Anuluj zmiany).

Administration > Factory Defaults (Administracja > Domyślne ustawienia fabryczne)

Ten ekran umożliwia przywrócenie domyślnych ustawień fabrycznych konfiguracji mostu.

Domyślne ustawienia fabryczne

Restore All Settings (Przywróć wszystkie ustawienia) Aby zresetować ustawienia mostu do wartości fabrycznych, kliknij przycisk **Restore All Settings** (Przywróć wszystkie ustawienia). Po przywróceniu ustawień domyślnych zostaną utracone wszelkie zapisane ustawienia.



Administration > Upgrade Firmware (Administracja > Uaktualnienie oprogramowania sprzętowego)

Ten ekran umożliwia uaktualnienie oprogramowania sprzętowego mostu. Oprogramowanie sprzętowe należy uaktualniać tylko wówczas, gdy występują problemy z mostem lub gdy nowa wersja oprogramowania sprzętowego zawiera funkcję interesującą użytkownika.



Przed uaktualnieniem oprogramowania sprzętowego pobierz plik uaktualnienia oprogramowania sprzętowego mostu z witryny firmy Linksys znajdującej się pod adresem **www.Linksys.com/support**.

Uaktualnienie oprogramowania sprzętowego

Please select a file to upgrade the firmware (Wybierz plik uaktualnienia oprogramowania sprzętowego) Kliknij przycisk **Browse** (Przeglądaj) i wybierz plik uaktualnienia oprogramowania sprzętowego. Następnie kliknij przycisk **Start to Upgrade** (Rozpocznij uaktualnianie) i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Status > Bridge (Stan > Most)

Wyświetlone zostaną informacje o aktualnym stanie mostu.



Bridge Information (Informacje o moście)

Firmware Version (Wersja oprogramowania sprzętowego) Wyświetlone zostaną informacje o aktualnej wersji oprogramowania sprzętowego mostu.

Sieć lokalna

Local MAC Address (Lokalny adres MAC) Wyświetlony zostanie adres MAC mostu, jaki widoczny jest w lokalnej sieci przewodowej Ethernet.

IP Address (Adres IP) Wyświetlony zostanie adres IP mostu, jaki widoczny jest w lokalnej sieci przewodowej Ethernet.

Subnet Mask (Maska podsieci) Wyświetlona zostanie maska podsieci skonfigurowana dla sieci lokalnej.

Status > Wireless (Stan > Połączenie bezprzewodowe)

Wyświetlone zostaną informacje o sieci bezprzewodowej.



Wireless (Połączenie bezprzewodowe)

Status (Stan) Wyświetlony zostanie stan połączenia z siecią bezprzewodową.

MAC Address (Adres MAC) Wyświetlony zostanie adres MAC mostu, jaki widoczny jest w lokalnej sieci bezprzewodowej.

Network Name (SSID) (Nazwa sieciowa (SSID)) Zostanie wyświetlona nazwa sieci bezprzewodowej lub identyfikator SSID.

BSSID Zostanie wyświetlony adres MAC połączonego routera bezprzewodowego (lub punktu dostępowego) w sieci bezprzewodowej.

Radio Band (Pasmo radiowe) Zostanie wyświetlone pasmo radiowe sieci bezprzewodowej.

Channel Width (Zasięg kanału) Zostanie wyświetlony zasięg kanału (w MHz) używany przez sieć bezprzewodową.

Wide Channel (Kanał dla całej sieci) Wyświetlony zostanie kanał dla całej sieci, zależnie od ustawień kanałów routera sieciowego. Jeśli dla opcji Radio Band (Pasmo radiowe) routera wybrano ustawienie Wide - 40MHz Channel (Dla całej sieci — kanał 40 MHz), będzie ono dostępne dla głównego kanału Wireless-N.

Standard Channel (Kanał standardowy) Zostanie wyświetlone ustawienie kanału standardowego. Jeśli dla opcji Radio Band (Pasmo radiowe) routera wybrano ustawienie Wide - 40MHz Channel (Dla całej sieci — kanał 40 MHz), kanał standardowy będzie kanałem pomocniczym dla standardu Wireless-N.

Bit Rate (Prędkość bitowa) Zostanie wyświetlona prędkość transmisji danych.

Signal (Sygnał) Wyświetlana jest procentowa siła sygnału. 100% oznacza najmocniejszą możliwą siłę sygnału, natomiast 0% oznacza najsłabszy możliwy sygnał.

Security (Zabezpieczenia) Zostaną wyświetlone informacje o metodzie zabezpieczeń używanej w sieci bezprzewodowej.

Rozwiązywanie problemów

WES610N/WET610N

Komputer lub inne przewodowe urządzenie Ethernet nie może nawiązać komunikacji z routerem bezprzewodowym.

1. Otwórz narzędzie WWW mostu.
2. Na ekranie *Basic Wireless Settings* (Podstawowe ustawienia sieci bezprzewodowej) upewnij się, że nazwa sieci (SSID) jest zgodna z nazwą sieci bezprzewodowej.
3. Upewnij się, że ustawienia zabezpieczeń (WPA, WPA2 lub WEP) są zgodne z ustawieniami zabezpieczeń sieci bezprzewodowej.

Należy zmienić adres IP mostu.

Jeśli most jest podłączony do sieci z serwerem DHCP (zazwyczaj jest nim router), to uzyskuje swój adres IP z tego serwera. W przypadku braku serwera DHCP most używa domyślnego, statycznego adresu IP **169.254.1.250**.

Jeśli most ma zawsze używać statycznego adresu IP, wykonaj następujące polecenia:

1. Otwórz narzędzie WWW mostu.
2. Kliknij kartę **Network Setup** (Konfiguracja sieci).
3. Z menu rozwijanego *Network Connection Type* (Typ połączenia sieciowego) wybierz opcję **Static IP** (Statyczny adres IP).
4. Wypełnij pola *Static IP Address* (Statyczny adres IP), *Subnet Mask* (Maska podsieci) oraz *Default Gateway* (Brama domyślna).
5. Kliknij przycisk **Save Settings** (Zapisz ustawienia).

Komputer lub inne przewodowe urządzenie Ethernet podłączone do routera nie może komunikować się z innymi urządzeniem podłączonym do sieci bezprzewodowej (takim jak komputer lub drukarka).

Sprawdź następujące możliwości:

- Upewnij się, że urządzenie podłączone do sieci bezprzewodowej znajduje się w tej samej sieci bezprzewodowej co komputer lub inne przewodowe urządzenie Ethernet podłączone do mostu.
- Upewnij się, że identyczna nazwa sieci bezprzewodowej (SSID) jest używana dla wszystkich urządzeń w sieci bezprzewodowej.
- Upewnij się, że wszystkie urządzenia znajdują się w tej samej sieci IP i używają zgodnych adresów IP.

Narzędzie WWW nie przyjmuje podanego hasła.

Sprawdź następujące możliwości:

- W haśle jest uwzględniana wielkość liter. Upewnij się, że wpisujesz hasło, korzystając ze znaków prawidłowej wielkości.
- W razie zapomnienia hasła można przywrócić domyślne ustawienia fabryczne mostu.

 W tym celu naciśnij przycisk **Reset** mostu i przytrzymaj go przez około 5 s. Zostanie przywrócone fabryczne hasło domyślne **admin**. Wszystkie pozostałe ustawienia mostu także zostaną zresetowane do fabrycznych wartości domyślnych (aby przejść do narzędzia WWW, wprowadź wyraz **admin** w polu *Password* (Hasło).

Nowe ustawienia wprowadzone za pośrednictwem narzędzia WWW nie są wyświetlane na ekranie.

Kliknij przycisk **Odśwież** w przeglądarce. Jeśli nowe ustawienia nie zostaną wyświetlone, wykonaj następujące polecenia:

1. Odłącz zasilacz sieciowy od mostu.
2. Odczekaj 5 sekund, a następnie podłącz ponownie zasilacz sieciowy do mostu.
3. Kliknij przycisk **Odśwież** w przeglądarce.

INTERNET
Jeśli w tym rozdziale nie ma odpowiedzi na określone pytanie, należy przejść na stronę internetową **Linksys.com/support**

Dane techniczne

WES610N

Model	WES610N
Standardy	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Diody LED	Zasilanie, Ethernet, Wi-Fi Protected Setup™, Sieć bezprzewodowa, połączenie i aktywność poszczególnych portów Ethernet
Porty	Ethernet (4), zasilanie
Przyciski	reset, bezpieczna konfiguracja Wi-Fi
Rodzaj okablowania	CAT5e
Anteny	3 (wewnętrzne)
Typ złącza antenowego	ND
Odłączane (Tak/Nie)	Nie
Modulacje	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Moc RF (EIRP) w dBm	802.11a: 15 dBm (typowa) przy 54 Mb/s 802.11b: 19 dBm (typowa) przy 11 Mb/s 802.11g: 16 dBm (typowa) przy 54 Mb/s 802.11n (2,4 GHz): 18 dBm (typowa) przy MCS15 802.11n (5 GHz): 16 dBm (typowa) przy MCS15
Czułość odbiornika	802.11a: -72 dBm (typowa) przy 54 Mb/s 802.11b: -85 dBm (typowa) przy 11 Mb/s 802.11g: -73 dBm (typowa) przy 54 Mb/s 802.11n (20 MHz): -75 dBm (typowa) przy MCS15 802.11n (40 MHz): -69 dBm (typowa) przy MCS15
Zysk anteny w dBi	1
Zabezpieczenia sieci bezprzewodowej	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Klucz zabezpieczeń zabezpieczeń	Szyfrowanie maks. 128-bitowe

Środowisko użytkowania

Wymiary	177 x 128 x 68 mm (6,97" x 5,04" x 2,68")
Waga	295 g (0,65 uncji)
Certyfikaty	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Zasilanie	12 V, 1 A
Temp. pracy	od 0 do 40°C (od 32 do 104°F)
Temp. przechowywania	od -20 do 60°C (od -4 do 140°F)
Wilgotność podczas pracy	od 10 do 85% (bez kondensacji)
Wilgotność podczas przechowywania	od 5 do 90% (bez kondensacji)

Dane techniczne mogą ulec zmianie bez powiadomienia.

WET610N

Model	WET610N
Standardy	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Diody LED	Zasilanie, Ethernet, Wi-Fi Protected Setup™, Sieć bezprzewodowa
Porty	Ethernet, zasilanie
Przyciski	reset, bezpieczna konfiguracja Wi-Fi
Rodzaj okablowania	CAT5e
Anteny	3 (wewnętrzne)
Typ złącza antenowego	ND
Odłączane (Tak/Nie)	Nie
Modulacje	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Moc RF (EIRP) w dBm	802.11a: 15 dBm (typowa) przy 54 Mb/s 802.11b: 18 dBm (typowa) przy 11 Mb/s 802.11g: 16 dBm (typowa) przy 54 Mb/s 802.11n: 12 dBm (typowa) przy 130 Mb/s (HT20), 270 Mb/s (HT40)
Czułość odbiornika	802.11a: -72 dBm (typowa) przy 54 Mb/s 802.11b: -85 dBm (typowa) przy 11 Mb/s 802.11g: -73 dBm (typowa) przy 54 Mb/s 802.11n: -70 dBm (typowa) przy MCS15/2,4 GHz, -69 dBm (typowa) przy MCS15/5,0 GHz
Zysk anteny w dBi	1
Zabezpieczenia sieci bezprzewodowej	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Klucz zabezpieczeń zabezpieczeń	Szyfrowanie maks. 128-bitowe

Środowisko użytkowania

Wymiary	145 x 106 x 52 mm (5,71" x 4,17" x 2,05")
Waga	159 g (5,61 uncji)
Certyfikaty	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Zasilanie	12 V, 1 A
Temp. pracy	od 0 do 40°C (od 32 do 104°F)
Temp. przechowywania	od -20 do 60°C (od -4 do 140°F)
Wilgotność podczas pracy	od 10 do 85% (bez kondensacji)
Wilgotność podczas przechowywania	od 5 do 90% (bez kondensacji)

Dane techniczne mogą ulec zmianie bez powiadomienia.

Linksys.com/support

Cisco, logo Cisco oraz Linksys są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Cisco i/lub jej spółek zależnych w Stanach Zjednoczonych i innych państwach.
Listę znaków towarowych firmy Cisco można znaleźć na stronie www.cisco.com/go/trademarks. Wszelkie inne znaki towarowe użyte w niniejszym dokumencie należą do odpowiednich właścicieli.

© 2011 Cisco i/lub jej spółki zależne. Wszelkie prawa zastrzeżone.

3425-01249



Manual do utilizador

Linksys WET610N/WES610N | Ponte de entretenimento N de banda dupla

Índice

Descrição geral do produto

Painel de LEDs 2
Painel das portas 3

Lista de verificação da segurança sem fios

Alterar o nome ou SSID predefinido da rede sem fios 4
Alterar a palavra-passe predefinida 4
Activar o filtro de endereços MAC 4
Activar a encriptação 4

Directrizes gerais de segurança da rede 4
Sugestões adicionais de segurança 5

Configuração avançada

Como aceder ao utilitário baseado no browser 6
Setup (Configuração) > Basic Setup (Configuração básica) 7
Idioma 7
Configuração da rede 7
Wireless (Sem fios) > Basic Wireless Settings (Definições sem fios básicas) 7
Definições sem fios básicas 8
Segurança sem fios 8
Wi-Fi Protected Setup 9
Wireless (Sem fios) > Wireless Network Site Survey (Pesquisa de sites de redes sem fios) 10
Pesquisa de sites de redes sem fios 10
Wireless (Sem fios) > WMM® 11
WMM 12
Wireless (Sem fios) > Advanced Wireless Settings (Definições sem fios avançadas) 13
Sem fios avançadas 14
Administration (Administração) > Management (Gestão) 14
Gestão 15
Administration (Administração) > Factory Defaults (Predefinições de fábrica) 15
Predefinições de fábrica 15
Administration (Administração) > Upgrade Firmware (Actualizar firmware) 15
Actualizar firmware 16
Status (Estado) > Bridge (Ponte) 16
Informações da ponte 16
Rede local 16
Status (Estado) > Wireless (Sem fios) 16
Sem fios 16

Resolução de problemas

WES610N/WET610N 17

Especificações

WES610N 18
WET610N 19

Descrição geral do produto

Obrigado por escolher a ponte de entretenimento N de banda dupla da Linksys. A ponte pode ligar qualquer dispositivo Ethernet com fios à sua rede sem fios. A ponte baseia-se na tecnologia sem fios N de banda dupla e, por isso, é compatível com qualquer router ou ponto de acesso sem fios N, G, A ou B. Para a primeira instalação, siga os passos presentes na pasta do CD. Para configurar as definições avançadas, utilize o conveniente utilitário baseado no browser.

Painel de LEDs



WES610N WET610N

Sem fios (Azul) O LED sem fios acende-se quando existe uma ligação sem fios. O LED fica intermitente quando a ponte está a enviar ou a receber activamente dados através da rede sem fios.

Botão Wi-Fi Protected Setup Se o seu router suportar Wi-Fi Protected Setup e utilizar a segurança WPA ou WPA2, poderá utilizar a função Wi-Fi Protected Setup para ligar automaticamente a ponte. Para utilizar a função Wi-Fi Protected Setup, consulte "Wireless (Sem fios) > Basic Wireless Settings (Definições sem fios básicas)" na página 7.

LED Wi-Fi Protected Setup (Azul/Âmbar) O LED fica intermitente a azul durante dois minutos, durante o processo de Wi-Fi Protected Setup. Acende-se a azul quando a segurança sem fios estiver activada. Se ocorrer um erro durante o processo de Wi-Fi Protected Setup, o LED acende-se a âmbar. Certifique-se de que o router da rede suporta Wi-Fi Protected Setup. Aguarde até que o LED se desligue e, em seguida, tente novamente.

Ethernet (Azul) O LED Ethernet acende-se quando existe uma ligação com fios. O LED fica intermitente quando a ponta está a enviar ou receber activamente dados através da porta Ethernet.

Alimentação (Azul) O LED de alimentação acende-se quando a ponte é ligada.

Painel das portas



WES610N WET610N

Ethernet A porta Ethernet liga a ponte a um computador ou outro dispositivo de rede Ethernet. O WES610N tem quatro portas e o WET610N tem uma única porta.

Reset (Repor) Existem duas formas de repor as predefinições de fábrica da ponte. Prima e mantenha premido o botão Reset (Repor) durante aproximadamente cinco segundos, ou restaure as predefinições a partir de Administration (Administração) > Factory Defaults (Predefinições de fábrica) no utilitário baseado no browser da ponte. O WES610N tem um botão Reset (Repor) na parte inferior e o WET610N tem um botão Reset (Repor) no painel das portas traseiro.

Alimentação A porta de alimentação liga a ponte ao transformador incluído.

Lista de verificação da segurança sem fios

As redes sem fios são convenientes e de fácil instalação e, por isso, estão a ser adoptadas a um ritmo acelerado pelos utilizadores que dispõem de Internet de alta velocidade em casa. Como a rede sem fios funciona através do envio de informações por ondas de rádio, poderá ser mais vulnerável a intrusões do que uma rede com fios tradicional. Como os sinais emitidos pelos telemóveis ou telefones sem fios, os sinais emitidos pela sua rede sem fios também podem ser interceptados. Uma vez que não é possível impedir fisicamente alguém de ligar à sua rede sem fios, é necessário efectuar alguns passos adicionais para manter a sua rede segura.

Alterar o nome ou SSID predefinido da rede sem fios

Os dispositivos sem fios têm um nome ou Identificador do Conjunto de Serviços (SSID) da rede sem fios predefinido de fábrica. Trata-se do nome da sua rede sem fios e pode ter até 32 caracteres. Os produtos sem fios da Linksys utilizam **linksys** como o nome predefinido da rede sem fios. Deverá alterar o nome da rede sem fios para algo único, para distinguir a sua rede sem fios de outras redes sem fios que possam existir em seu redor, mas não utilize informações pessoais (como o seu número da Segurança Social) porque estas informações poderão ficar disponíveis para qualquer pessoa que esteja à procura de redes sem fios.

Alterar a palavra-passe predefinida

Para os produtos sem fios como pontos de acesso e routers, será solicitada uma palavra-passe quando pretender alterar as respectivas definições. Estes dispositivos têm uma palavra-passe predefinida de fábrica. A palavra-passe predefinida da Linksys é **admin**. Os piratas informáticos conhecem estas predefinições e poderão tentar utilizá-las para aceder ao seu dispositivo sem fios e alterar as suas definições da rede. Para impedir qualquer alteração não autorizada, personalize a palavra-passe do dispositivo de modo a que seja difícil de adivinhar.

Activar o filtro de endereços MAC

Os routers da Linksys permitem-lhe activar o filtro de endereços MAC (Controlo de acesso a suportes de dados). O endereço MAC é uma série única de números e letras atribuída a cada dispositivo da rede. Com o filtro de endereços MAC activado, o acesso à rede sem fios é fornecido apenas para os dispositivos sem fios com endereços MAC específicos. Por exemplo, pode especificar o endereço MAC de cada computador presente na sua casa para que apenas esses computadores possam aceder à sua rede sem fios.

Activar a encriptação

A encriptação protege os dados transmitidos numa rede sem fios. Wi-Fi Protected Access (WPA/WPA2) e Wired Equivalent Privacy (WEP) oferecem diferentes níveis de segurança para a comunicação sem fios.

Uma rede com encriptação WPA/WPA2 é mais segura do que uma rede com encriptação WEP, porque a WPA/WPA2 utiliza a encriptação de chaves dinâmicas. Para proteger as informações durante a transmissão através das ondas de rádio, deverá activar o nível mais alto de encriptação suportado pelo seu equipamento de rede.

WEP é uma norma de encriptação mais antiga e poderá ser a única opção disponível em alguns dispositivos mais antigos que não suportam WPA.

Directrizes gerais de segurança da rede

A segurança da rede sem fios é inútil se a rede subjacente não for segura.

- Proteja todos os computadores na rede com uma palavra-passe e proteja individualmente os ficheiros importantes com uma palavra-passe.
- Altere regularmente as palavras-passe.
- Instale software antivírus e software de firewall pessoal.
- Desactive a partilha de ficheiros (unidade a unidade). Algumas aplicações podem abrir a partilha de ficheiros sem o seu consentimento e/ou conhecimento.

Sugestões adicionais de segurança

- Mantenha os routers, pontos de acesso ou gateways sem fios afastados das paredes exteriores e das janelas.
- Desligue os routers, pontos de acesso ou gateways sem fios quando não estiverem a ser utilizados (à noite, durante as férias).
- Utilize frases-passe complexas com, pelo menos, oito caracteres. Combine letras e números para evitar utilizar palavras normais que podem ser encontradas no dicionário.

Configuração avançada

A ponte estará pronta para ser utilizada depois de ter sido configurada com os passos apresentados na pasta do CD. Contudo, se pretender alterar as respectivas definições avançadas, utilize o utilitário baseado no browser da ponte. Este capítulo descreve cada uma das páginas Web do utilitário, bem como as funções chave de cada página. O utilitário pode ser acedido através do browser de um computador ligado em rede com a ponte.

O utilitário baseado no browser tem os seguintes separadores principais: Setup (Configuração), Wireless (Sem fios), Administration (Administração) e Status (Estado). Estarão disponíveis separadores adicionais depois de clicar num dos separadores principais.

Como aceder ao utilitário baseado no browser

Utilize um browser para aceder ao utilitário baseado no browser.

Se a ponte estiver ligada a uma rede com um servidor DHCP (normalmente, o router da rede), a ponte obterá o respectivo endereço IP a partir do servidor DHCP. Se não existir nenhum servidor DHCP, a ponte utilizará o seu endereço IP estático predefinido, **169.254.1.250**. (Se definiu um endereço IP estático permanente na ponte através do utilitário baseado no browser, introduza o endereço IP estático.)

NOTA
Se não souber o endereço IP da ponte, poderá encontrá-lo na tabela de clientes DHCP do seu router. (Consulte a documentação do seu router.)

Se não conseguir localizar o endereço IP da ponte, poderá repor a ponte; prima o botão **Reset** (Repor) na ponte durante aproximadamente cinco segundos, utilizando um clipe aberto. As predefinições de fábrica da ponte serão repostas. A ponte pedirá um endereço IP ao servidor DHCP (normalmente, o router da rede). Se não for encontrado nenhum servidor DHCP, a ponte utilizará o seu endereço IP estático predefinido, **169.254.1.250**, até detectar um servidor DHCP que lhe atribua um endereço IP dinâmico.

Se a ponte não estiver associada a um router e estiver a utilizar as predefinições de fábrica, ligue um computador à ponte utilizando uma ligação Ethernet para aceder ao utilitário-baseado na Web. Terá de configurar a ligação Ethernet no computador com um endereço IP estático e uma máscara de sub-rede.

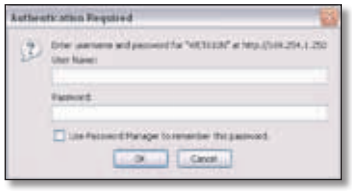
O endereço IP do seu adaptador Ethernet deve ser definido para um endereço IP específico.

1. No campo *IP address* (Endereço IP), introduza **169.254.x.y** (o "x" deve ser substituído por um número entre 1 e 254 e o "y" deve ser substituído por um número entre 0 e 255).
2. No campo *Subnet mask* (Máscara de sub-rede), introduza **255.255.0.0**.

NOTA
Os passos necessários para atribuir um endereço IP ao adaptador Ethernet no seu computador variam consoante o sistema operativo. Para obter instruções, consulte a documentação de ajuda do seu sistema operativo específico.

Depois de atribuir um endereço IP estático ao seu adaptador Ethernet, inicie o browser e introduza o endereço IP do adaptador (a predefinição é **169.254.1.250**) no campo *Address* (Endereço). Prima **Enter**.

É apresentado um ecrã a solicitar a palavra-passe. (Será apresentado um ecrã semelhante aos utilizadores que não utilizam o sistema operativo Windows XP.) Deixe o campo *User name* (Nome de utilizador) em branco. Introduza a palavra-passe que criou durante o Assistente de configuração. Se não tiver criado uma nova palavra-passe, utilize a palavra-passe predefinida **admin**. (Poderá definir uma nova palavra-passe a partir do ecrã *Administration* (Administração) > *Management* (Gestão). Clique em **OK** para continuar.



NOTA
Se não for apresentado o ecrã a solicitar a palavra-passe, aguarde dois minutos e tente novamente.

Setup (Configuração) > Basic Setup (Configuração básica)

O primeiro ecrã apresentado é o ecrã *Basic Setup* (Configuração básica). Utilize este ecrã para alterar o idioma do utilitário baseado no browser, ou para alterar as definições da rede Ethernet com fios da ponte.





Idioma

Language (Idioma) É utilizado para definir o idioma apresentado pelo utilitário baseado no browser. Seleccione o idioma pretendido no menu pendente.

Configuração da rede

Esta secção determina se o endereço IP da ponte é obtido automaticamente a partir de um servidor DHCP, como, por exemplo, o seu router da rede (Automatic Configuration - DHCP (Configuração automática - DHCP)), ou se é definido manualmente (Static IP (IP estático)).

Bridge IP (IP da ponte) Se a sua rede tiver um servidor DHCP, como, por exemplo, o seu router da rede, a atribuir endereços IP aos seus dispositivos da rede, mantenha a predefinição, **Automatic Configuration - DHCP** (Configuração automática - DHCP). A ponte pedirá um endereço IP ao servidor DHCP (normalmente, o router da rede). Se não for encontrado nenhum servidor DHCP, a ponte utilizará o seu endereço IP estático predefinido, **169.254.1.250**, até detectar um servidor DHCP que lhe atribua um endereço IP dinâmico.

Se pretender definir um endereço IP estático permanente para a ponte, seleccione **Static IP** (IP estático).

Se seleccionar Static IP (IP estático), preencha os seguintes campos:

- **Static IP Address** (Endereço IP estático) Introduza um endereço IP único que será utilizado para aceder ao utilitário baseado no browser.
- **Subnet Mask** (Máscara de sub-rede) Introduza a máscara de sub-rede da sua rede com fios.
- **Default Gateway** (Gateway predefinido) Introduza o endereço IP do gateway predefinido da sua rede (na maioria dos casos, é o seu router).

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Wireless (Sem fios) > Basic Wireless Settings (Definições sem fios básicas)

Utilize o ecrã *Basic Wireless Settings* (Definições sem fios básicas) para configurar as definições básicas sem fios e de segurança da ponte.

Existem duas formas de configurar as definições da ponte: manual e Wi-Fi Protected Setup. Wi-Fi Protected Setup é uma função que facilita a configuração da sua rede sem fios. Se o seu router da rede suportar Wi-Fi Protected Setup e utilizar a segurança WPA ou WPA2, poderá utilizar a função Wi-Fi Protected Setup para ligar automaticamente a ponte.

Configuration View (Vista da configuração) Para configurar manualmente a sua rede sem fios, seleccione **Manual**. Consulte **Definições sem fios básicas**, **página 8**. Para utilizar Wi-Fi Protected Setup, seleccione **Wi-Fi Protected Setup**. Consulte **Wi-Fi Protected Setup**, **página 9**.

Definições sem fios básicas



Network Name (SSID) (Nome da rede (SSID)) O SSID é o nome da rede partilhado entre todos os pontos de uma rede sem fios. O SSID tem de ser idêntico para todos os dispositivos da rede sem fios. É sensível a maiúsculas e não pode exceder 32 caracteres (utilize qualquer carácter do teclado). Certifique-se de que esta definição corresponde à definição no seu router sem fios ou ponte de acesso. Para obter segurança adicional, deverá alterar o SSID predefinido (**linksys**) para um nome único.

Segurança sem fios

A ponte suporta as seguintes opções de segurança sem fios: WPA Personal, WPA2 Personal e WEP. O WPA (Wi-Fi Protected Access) e o WPA2 são métodos de segurança mais fortes do que o WEP (Wired Equivalent Privacy). Para obter mais informações sobre a segurança sem fios, consulte "Lista de verificação da segurança sem fios", página 4.

Modo de segurança

Seleccione o método de segurança para a sua rede sem fios. Se não pretender utilizar a segurança sem fios, mantenha a predefinição, **Disabled** (Desactivado).

NOTA
Tenha em atenção que todos os dispositivos na sua rede sem fios TÊM de utilizar o mesmo método de segurança e frase-passe/chave, pois, caso contrário, os dispositivos sem fios não conseguirão comunicar entre si.

WPA Personal

WPA é uma norma de segurança mais forte do que a encriptação WEP.



Encryption (Encriptação) O WPA suporta o método de encriptação TKIP, com chaves de encriptação dinâmicas.

Passphrase (Frase-passe) Introduza a chave partilhada pela ponte e pelo seu router sem fios ou ponto de acesso. Tem de ter entre 8 e 63 caracteres.

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

WPA2 Personal

O WPA2 é uma versão mais avançada e mais segura do WPA.



Encryption (Encriptação) O WPA2 suporta dois métodos de encriptação, TKIP e AES, com chaves de encriptação dinâmicas. Seleccione o método de encriptação, **AES** ou **TKIP or AES** (TKIP ou AES). A selecção predefinida é **AES**.

Passphrase (Frase-passe) Introduza a chave partilhada pela ponte e pelo router sem fios ou ponto de acesso. Tem de ter entre 8 e 63 caracteres.

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

WEP

O WEP é um método de encriptação básico, que não é tão seguro como o WPA ou o WPA2.



Encryption (Encriptação) Seleccione um nível de encriptação WEP, **40/64 bits (10 hex digits)** (40/64 bits (10 dígitos hexadecimais)) ou **104/128 bits (26 hex digits)** (104/128 bits (26 dígitos hexadecimais)). A predefinição é **40/64 bits (10 hex digits)** (40/64 bits (10 dígitos hexadecimais)).

Key 1 (Chave 1) Introduza a chave WEP da sua rede.

Tx Key (Chave Tx) **Key 1** (Chave 1) é a chave de transmissão utilizada pela ponte.

Authentication (Autenticação) A predefinição é **Auto** (Automático), que permite a utilização da autenticação Sistema aberto ou Chave partilhada. Seleccione **Open** (Aberto) para utilizar a autenticação Sistema aberto; o remetente e o destinatário não utilizam uma chave WEP para a autenticação. Seleccione **Shared** (Partilhada) para utilizar a autenticação Chave partilhada; o remetente e o destinatário utilizam uma chave WEP para a autenticação.

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Wi-Fi Protected Setup

Estão disponíveis dois métodos. Utilize o método que se aplica ao router que está a utilizar.





Método n.º 1

Utilize este método se o seu router tiver um botão Wi-Fi Protected Setup.

1. Clique ou prima o botão **Wi-Fi Protected Setup** no router.
2. No espaço de dois minutos, clique no botão **Wi-Fi Protected Setup** no ecrã *Wi-Fi Protected Setup* da ponte.
3. Depois de a ponte ter sido configurada, clique em **Close** (Fechar).

O ecrã *Wi-Fi Protected Setup* apresenta o estado da ligação, o nome da rede (SSID) e o método de segurança.

Método n.º 2

Utilize este método se o seu router solicitar o número PIN da ponte.

1. No ecrã *Wi-Fi Protected Setup* do **router**, introduza o número PIN no ecrã *Wi-Fi Protected Setup* da **ponte**. Em seguida, clique em **Register** (Registar) ou no botão apropriado. (Também está indicado na etiqueta existente na parte inferior da ponte.)
2. No ecrã *Wi-Fi Protected Setup* da **ponte**, clique em **OK**.
3. Depois de a ponte ter sido configurada, clique em **Close** (Fechar).

O ecrã *Wi-Fi Protected Setup* apresenta o estado da ligação, o nome da rede (SSID) e o método de segurança.

Wireless (Sem fios) > Wireless Network Site Survey (Pesquisa de sites de redes sem fios)

Clique no separador **Wireless Network Site Survey** (Pesquisa de sites de redes sem fios) para iniciar uma pesquisa de sites. O ecrã *Wireless Network Site Survey* (Pesquisa de sites de redes sem fios) indica as redes sem fios detectadas pela ponte.



Pesquisa de sites de redes sem fios

Number of Wireless Networks (Número de redes sem fios) É apresentado o número de redes sem fios detectados pela ponte.

Select (Seleccionar) Para ligar a uma rede sem fios, clique em **Select** (Seleccionar). Em seguida, clique em **Connect** (Ligar).

Wireless Network Name (Nome da rede sem fios) É apresentado o nome ou SSID da rede sem fios.

GHz É apresentada a banda de rádio da rede sem fios.

Signal (Sinal) É apresentada a percentagem da potência do sinal. 100% é a potência do sinal mais forte possível; 0% é a mais fraca.

Security (Segurança) Se a rede suportar Wi-Fi Protected Setup, é apresentado o ícone da função Wi-Fi Protected Setup . É apresentado o método de segurança utilizado pela rede sem fios.

Clique em **Refresh** (Actualizar) para actualizar as informações apresentadas no ecrã.

Depois de seleccionar uma rede, clique em **Connect** (Ligar). É apresentado um novo ecrã. Siga as instruções relativas ao método de segurança da sua rede.

WPA



Network Name (SSID) (Nome da rede (SSID)) É automaticamente apresentado o nome da rede seleccionada.

Security Mode (Modo de segurança) É automaticamente apresentado o WPA Personal.

Encryption (Encriptação) O WPA suporta o método de encriptação TKIP, com chaves de encriptação dinâmicas.

Passphrase (Frase-passe) Introduza a chave partilhada pela ponte e pelo router sem fios ou ponto de acesso. Tem de ter entre 8 e 63 caracteres.

Clique em **Refresh** (Actualizar) para actualizar as informações apresentadas no ecrã.

Depois de introduzir as definições de segurança, clique em **Connect** (Ligar).

WPA2



Network Name (SSID) (Nome da rede (SSID)) É automaticamente apresentado o nome da rede seleccionada.

Security Mode (Modo de segurança) É automaticamente apresentado o WPA2 Personal.

Encryption (Encriptação) O WPA2 suporta dois métodos de encriptação, TKIP e AES, com chaves de encriptação dinâmicas. Seleccione o método de encriptação, **AES** ou **TKIP or AES** (TKIP ou AES).

Passphrase (Frase-passe) Introduza a chave partilhada pela ponte e pelo router sem fios ou ponto de acesso. Tem de ter entre 8 e 63 caracteres.

Clique em **Refresh** (Actualizar) para actualizar as informações apresentadas no ecrã.

Depois de introduzir as definições de segurança, clique em **Connect** (Ligar).

WEP



Network Name (SSID) (Nome da rede (SSID)) É automaticamente apresentado o nome da rede seleccionada.

Security Mode (Modo de segurança) É automaticamente apresentado o WEP.

Encryption (Encriptação) Seleccione um nível de encriptação WEP, **40/64 bits (10 hex digits)** (40/64 bits (10 dígitos hexadecimais)) ou **104/128 bits (26 hex digits)** (104/128 bits (26 dígitos hexadecimais).

Key 1 (Chave 1) Introduza a chave WEP da sua rede.

Tx Key (Chave Tx) **Key 1** (Chave 1) é a chave de transmissão utilizada pela ponte.

Authentication (Autenticação) A predefinição é **Auto** (Automático), que permite a utilização da autenticação Sistema aberto ou Chave partilhada. Seleccione **Open** (Aberto) para utilizar a autenticação Sistema aberto; o remetente e o destinatário não utilizam uma chave WEP para a autenticação. Seleccione **Shared** (Partilhada) para utilizar a autenticação Chave partilhada; o remetente e o destinatário utilizam uma chave WEP para a autenticação.

Clique em **Refresh** (Actualizar) para actualizar as informações apresentadas no ecrã.

Depois de introduzir as definições de segurança, clique em **Connect** (Ligar).

Wireless (Sem fios) > WMM®

Configure as definições de Wireless MultiMedia (WMM). O WMM atribui prioridade aos pacotes consoante o respectivo modo de acesso (tipo de tráfego): Background (Segundo plano), Best Effort (Melhor esforço), Video (Vídeo) ou Voice (Voz). Estas definições só devem ser ajustadas por um administrador experiente, uma vez que definições incorrectas poderão reduzir o desempenho da rede sem fios.



NOTA
As definições no ecrã *WMM* destinam-se apenas a utilizadores avançados.

WMM

Modo de acesso

Pode atribuir definições diferentes aos quatro modos de acesso disponíveis. Seleccione o modo que pretende configurar: **Background** (Segundo plano), **Best Effort** (Melhor esforço), **Video** (Vídeo) ou **Voice** (Voz). Siga as instruções relativas ao modo seleccionado.

Segundo plano

Use Aggregation (Utilizar agregação) Esta opção define se a camada de MAC (Controlo de acesso a suportes de dados) configura ou não uma sessão de ADDBA (Adicionar confirmação do bloco). A predefinição é **No** (Não). Seleccione **Yes** (Sim) para activar esta opção.

Accept Aggregation (Aceitar agregação) Esta opção define se a camada MAC aceita ou não um pedido de ADDBA. A predefinição é **Yes** (Sim). Seleccione **No** (Não) para desactivar esta opção.

Max. Number of Packets in Aggregation (Número máx. de pacotes na agregação) Esta opção define o número máximo de pacotes (subpacotes) na agregação. O intervalo é de **0** a **7**. A predefinição é **7**.

Max. Aggregation Size (Tamanho máx. da agregação) Esta opção define o tamanho máximo da agregação (em bytes). O intervalo é de **0** a **16000**. A predefinição é **12000**.

Timeout Internal (Intervalo de tempo limite) Esta opção define o período de tempo limite no qual a agregação deve ser fechada com uma "condição de fecho" antes de ser fechada pelo temporizador. O intervalo é de **0** a **100** ms. A predefinição é **3**.

Min. Size of Packet in Aggregation (Tamanho mín. dos pacotes na agregação) Esta opção define o tamanho mínimo (em bytes) dos pacotes acumulados na agregação. O intervalo é de **0** a **1500**. A predefinição é **10**.

ADDBA Timeout (Tempo limite de ADDBA) Esta opção define o período de tempo após o qual a configuração de ADDBA é terminada, se não existirem trocas de pacotes pelo acordo de Confirmação do bloco (ACK) durante este período de tempo. O intervalo é de **0** a **65535** ms. A predefinição é **0**, que desactiva o tempo limite.

Aggregation Window Size (Tamanho da janela de agregação) Esta opção define o número máximo de pacotes transmitidos sem obter ACKs. O intervalo é de **0** a **64**. A predefinição é **64**.

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Melhor esforço

Use Aggregation (Utilizar agregação) Esta opção define se a camada de MAC (Controlo de acesso a suportes de dados) configura ou não uma sessão de ADDBA (Adicionar confirmação do bloco). A predefinição é **Yes** (Sim). Seleccione **No** (Não) para desactivar esta opção.

Accept Aggregation (Aceitar agregação) Esta opção define se a camada MAC aceita ou não um pedido de ADDBA. A predefinição é **Yes** (Sim). Seleccione **No** (Não) para desactivar esta opção.

Max. Number of Packets in Aggregation (Número máx. de pacotes na agregação) Esta opção define o número máximo de pacotes (subpacotes) na agregação. O intervalo é de **0** a **10**. A predefinição é **10**.

Max. Aggregation Size (Tamanho máx. da agregação) Esta opção define o tamanho máximo da agregação (em bytes). O intervalo é de **0** a **20000**. A predefinição é **16000**.

Timeout Internal (Intervalo de tempo limite) Esta opção define o período de tempo limite no qual a agregação deve ser fechada com uma "condição de fecho" antes de ser fechada pelo temporizador. O intervalo é de **0** a **100** ms. A predefinição é **3**.

Min. Size of Packet in Aggregation (Tamanho mín. dos pacotes na agregação) Esta opção define o tamanho mínimo (em bytes) dos pacotes acumulados na agregação. O intervalo é de **0** a **1500**. A predefinição é **10**.

ADDBA Timeout (Tempo limite de ADDBA) Esta opção define o período de tempo após o qual a configuração de ADDBA é terminada, se não existirem trocas de pacotes pelo acordo de Confirmação do bloco (ACK) durante este período de tempo. O intervalo é de **0** a **65535** ms. A predefinição é **0**, que desactiva o tempo limite.

Aggregation Window Size (Tamanho da janela de agregação) Esta opção define o número máximo de pacotes transmitidos sem obter ACKs. O intervalo é de **0** a **64**. A predefinição é **64**.

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Vídeo

Use Aggregation (Utilizar agregação) Esta opção define se a camada de MAC (Controlo de acesso a suportes de dados) configura ou não uma sessão de ADDBA (Adicionar confirmação do bloco). A predefinição é **Yes** (Sim). Seleccione **No** (Não) para desactivar esta opção.

Accept Aggregation (Aceitar agregação) Esta opção define se a camada MAC aceita ou não um pedido de ADDBA. A predefinição é **Yes** (Sim). Seleccione **No** (Não) para desactivar esta opção.

Max. Number of Packets in Aggregation (Número máx. de pacotes na agregação) Esta opção define o número máximo de pacotes (subpacotes) na agregação. O intervalo é de **0** a **7**. A predefinição é **7**.

Max. Aggregation Size (Tamanho máx. da agregação) Esta opção define o tamanho máximo da agregação (em bytes). O intervalo é de **0** a **16000**. A predefinição é **12000**.

Timeout Internal (Intervalo de tempo limite) Esta opção define o período de tempo limite no qual a agregação deve ser fechada com uma "condição de fecho" antes de ser fechada pelo temporizador. O intervalo é de **0** a **100** ms. A predefinição é **3**.

Min. Size of Packet in Aggregation (Tamanho mín. dos pacotes na agregação) Esta opção define o tamanho mínimo (em bytes) dos pacotes acumulados na agregação. O intervalo é de **0** a **1500**. A predefinição é **10**.

ADDBA Timeout (Tempo limite de ADDBA) Esta opção define o período de tempo após o qual a configuração de ADDBA é terminada, se não existirem trocas de pacotes pelo acordo de Confirmação do bloco (ACK) durante este período de tempo. O intervalo é de **0** a **65535** ms. A predefinição é **0**, que desactiva o tempo limite.

Aggregation Window Size (Tamanho da janela de agregação) Esta opção define o número máximo de pacotes transmitidos sem obter ACKs. O intervalo é de **0** a **64**. A predefinição é **64**.

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Voz

Use Aggregation (Utilizar agregação) Esta opção define se a camada de MAC (Controlo de acesso a suportes de dados) configura ou não uma sessão de ADDBA (Adicionar confirmação do bloco). A predefinição é **Yes** (Sim). Seleccione **No** (Não) para desactivar esta opção.

Accept Aggregation (Aceitar agregação) Esta opção define se a camada MAC aceita ou não um pedido de ADDBA. A predefinição é **Yes** (Sim). Seleccione **No** (Não) para desactivar esta opção.

Max. Number of Packets in Aggregation (Número máx. de pacotes na agregação) Esta opção define o número máximo de pacotes (subpacotes) na agregação. O intervalo é de **0** a **2**. A predefinição é **2**.

Max. Aggregation Size (Tamanho máx. da agregação) Esta opção define o tamanho máximo da agregação (em bytes). O intervalo é de **0** a **16000**. A predefinição é **10000**.

Timeout Internal (Intervalo de tempo limite) Esta opção define o período de tempo limite no qual a agregação deve ser fechada com uma "condição de fecho" antes de ser fechada pelo temporizador. O intervalo é de **0** a **100** ms. A predefinição é **10**.

Min. Size of Packet in Aggregation (Tamanho mín. dos pacotes na agregação) Esta opção define o tamanho mínimo (em bytes) dos pacotes acumulados na agregação. O intervalo é de **0** a **1500**. A predefinição é **10**.

ADDBA Timeout (Tempo limite de ADDBA) Esta opção define o período de tempo após o qual a configuração de ADDBA é terminada, se não existirem trocas de pacotes pelo acordo de Confirmação do bloco (ACK) durante este período de tempo. O intervalo é de **0** a **65535** ms. A predefinição é **0**, que desactiva o tempo limite.

Aggregation Window Size (Tamanho da janela de agregação) Esta opção define o número máximo de pacotes transmitidos sem obter ACKs. O intervalo é de **0** a **64**. A predefinição é **64**.

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Wireless (Sem fios) > Advanced Wireless Settings (Definições sem fios avançadas)

Configure as funções sem fios avançadas da ponte. Estas definições só devem ser ajustadas por um administrador experiente, uma vez que definições incorrectas poderão reduzir o desempenho da rede sem fios.



NOTA
As definições no ecrã *Advanced Wireless Settings* (Definições sem fios avançadas) destinam-se apenas a utilizadores avançados.

Sem fios avançadas

Use LDPC (Utilizar LDPC) O LPDC (Código de verificação de paridade de baixa densidade) activa ou desactiva a correcção de erros para reduzir a probabilidade de perda de dados em canais ruidosos. O algoritmo de adaptação da velocidade desactiva automaticamente a codificação LDPC quando estão a ser utilizadas velocidades PHY elevadas (superiores a 162). Para utilizar o esquema de correcção de erros avançado do LDCP, mantenha a predefinição, **Yes** (Sim). Caso contrário, seleccione **No** (Não).

ERP Protection Type (Tipo de protecção ERP) Esta opção configura a protecção dos pacotes OFDM apesar da presença de estações 802.11b na rede sem fios. Através do envio de pacotes RTS/CTS ou CTS2Self a velocidades de 802.11b, a ponte informa a rede sem fios de que vão ser transferidos pacotes OFDM e protege os pacotes na rede sem fios. Os pacotes RTS/CTS e CTS2Self criam sobrecarga, o que pode resultar em débitos inferiores.

A opção RTS/CTS fornece uma melhor cobertura mas débitos inferiores em comparação com a CTS2Self, porque a opção RTS/CTS inclui a confirmação por parte do dispositivo receptor. Para utilizar a opção RTS/CTS, mantenha a predefinição, **RTS/CTS**. A opção None (Nenhum) pode causar colisões entre os pacotes OFDM e CCK. Para utilizar a opção None (Nenhum), seleccione **None** (Nenhum). Para utilizar a opção CTS2Self, seleccione **CTS2Self**.

11n Protection Type (Tipo de protecção 11n) Esta opção configura a protecção a partir dos dispositivos não HT (Alto débito) na rede sem fios. No caso de o router sem fios (ou ponto de acesso) detectar uma associação de um dispositivo não HT já existente, informará todos os dispositivos HT para utilizarem os mecanismos RTS/CTS ou CTS2Self antes de cada transmissão de dados. Esta função também suporta todas as protecções da norma 802.11n, incluindo o MIMO.

A opção RTS/CTS fornece uma melhor cobertura mas débitos inferiores em comparação com a CTS2Self, porque a opção RTS/CTS inclui a confirmação por parte do dispositivo receptor. Para utilizar a opção RTS/CTS, mantenha a predefinição, **RTS/CTS**. A opção None (Nenhum) pode causar colisões entre os pacotes HT e os já existentes. Para utilizar a opção None (Nenhum), seleccione **None** (Nenhum). Para utilizar a opção CTS2Self, seleccione **CTS2Self**.

Percentage of maximal transmit power (Percentagem da potência de transmissão máxima) Esta opção define a percentagem da potência de transmissão máxima em relação às restrições do domínio de regulamentação. Por exemplo, se a restrição do domínio de regulamentação permitir transmissões até 20 dB, a definição da percentagem para 50% permite uma potência de transmissão máxima de 10 dB. Seleccione a percentagem que pretende utilizar: **12%**, **25%**, **50%**ou **100%**. A predefinição é **100%**.

QoS Classification Type (Tipo de classificação de QoS) Esta opção define o mapeamento de 802.1D ou 802.1Q do campo DSCP/TOS IP para as prioridades de WMM (Background (Segundo plano), Best Effects (Melhores efeitos), Video (Vídeo), Voice (Voz)). Mantenha a predefinição, **802.1D** ou seleccione **802.1Q**, que é utilizado por algumas transmissões de IPTV.

Re-establish Ethernet connection when initiating wireless connection (Restabelecer a ligação Ethernet quando iniciar a ligação sem fios) Para activar a descoberta de DHCP a partir do dispositivo que reside na ponte, a ponte irá repor a ligação Ethernet entre a ponte e o dispositivo sempre uma ligação sem fios for estabelecida. Para desactivar este comportamento, seleccione **No** (Não). Caso contrário, mantenha a predefinição, **Yes** (Sim).

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Administration (Administração) > Management (Gestão)

Utilize este ecrã para gerir funções da ponte específicas: acesso ao utilitário-baseado na Web, cópia de segurança do ficheiro de configuração e reinicialização.



Gestão

Acesso à ponte

Utilize uma palavra-passe para proteger o acesso ao utilitário baseado no browser.

Bridge Password (Palavra-passe da ponte) Introduza uma nova palavra-passe para a ponte.

Re-enter to confirm (Introduza novamente para confirmar) Introduza novamente a palavra-passe para a confirmar.

Idle Timeout (Tempo limite de inactividade) O tempo de sessão é excedido após um período de inactividade especificado pelo utilizador. O intervalo é de **60** a **3600** segundos. A predefinição é **600**.

Acesso à Web

Access via Wireless (Acesso sem fios) Se estiver a utilizar a ponte num domínio público onde esteja a dar acesso sem fios aos seus convidados, poderá desactivar o acesso sem fios ao utilitário baseado no browser da ponte. Só conseguirá aceder ao utilitário baseado no browser através de uma ligação com fios se desactivar a definição. Mantenha a predefinição, **Enabled** (Activado) para permitir o acesso sem fios ao utilitário baseado na Web da ponte ou seleccione **Disabled** (Desactivado) para bloquear o acesso sem fios ao utilitário.

Cópia de segurança e restauro

Backup (Cópia de segurança) Para efectuar uma cópia de segurança do ficheiro de configuração da ponte, clique em **Backup Configurations** (Configurações de cópia de segurança). Em seguida, siga as instruções apresentadas no ecrã.

Restore (Restaurar) Clique em **Browse** (Procurar) e seleccione o ficheiro de configuração. Em seguida, clique em **Restore Configurations** (Restaurar configurações).

Reinicialização do sistema

Reboot (Reiniciar) Para reiniciar a ponte, clique em **Start to Reboot** (Iniciar reinicialização).

Clique em **Save Settings** (Guardar definições) para aplicar as suas alterações, ou clique em **Cancel Changes** (Cancelar alterações) para cancelar as suas alterações.

Administration (Administração) > Factory Defaults (Predefinições de fábrica)

Utilize este ecrã para restaurar a configuração da ponte para as suas predefinições de fábrica.

Predefinições de fábrica

Restore All Settings (Restaurar todas as definições) Para repor as definições da ponte para as predefinições de fábrica, clique em **Restore All Settings** (Restaurar todas as definições). Quaisquer definições que tenha guardado serão perdidas quando as predefinições forem restauradas.



Administration (Administração) > Upgrade Firmware (Actualizar firmware)

Utilize este ecrã para actualizar o firmware da ponte. Não actualize o firmware, a menos que ocorram problemas com a ponte ou que o novo firmware tenha uma função que pretenda utilizar.



Antes de actualizar o firmware, transfira o ficheiro de actualização do firmware da ponte a partir do site da Linksys, **www.Linksys.com/support**.

Actualizar firmware

Please select a file to upgrade the firmware (Seleccione um ficheiro para actualizar o firmware) Clique em **Browse** (Procurar) e seleccione o ficheiro de actualização do firmware. Em seguida, clique em **Start to Upgrade** (Iniciar actualização) e siga as instruções apresentadas no ecrã.

Status (Estado) > Bridge (Ponte)

São apresentadas as informações de estado actuais da ponte.



Informações da ponte

Firmware Version (Versão do firmware) É apresentado o firmware actual da ponte.

Rede local

Local MAC Address (Endereço MAC local) É apresentado o endereço MAC da ponte, conforme é mostrado na sua rede Ethernet local.

IP Address (Endereço IP) É apresentado o endereço IP da ponte, conforme é mostrado na sua rede Ethernet local.

Subnet Mask (Máscara de sub-rede) É apresentada a máscara de sub-rede configurada para a sua rede local.

Status (Estado) > Wireless (Sem fios)

São apresentadas informações sobre a sua rede sem fios.



Sem fios

Link Status (Estado da ligação) É apresentado o estado da ligação à sua rede sem fios.

MAC Address (Endereço MAC) É apresentado o endereço MAC da ponte, conforme é mostrado na sua rede sem fios local.

Network Name (SSID) (Nome da rede (SSID)) É apresentado o nome ou SSID da rede sem fios.

BSSID É apresentado o endereço MAC sem fios do router (ou ponto de acesso) sem fios ligado.

Radio Band (Banda de rádio) É apresentada a banda de rádio da sua rede sem fios.

Channel Width (Largura do canal) É apresentada a largura do canal, em MHz, utilizada pela sua rede sem fios.

Wide Channel (Canal de banda larga) Dependendo das definições de canal do seu router da rede, é apresentado o canal de banda larga. Se seleccionou Wide - 40MHz Channel (Banda larga - Canal de 40MHz) para a definição Radio Band (Banda de rádio) ou Channel Width (Largura do canal) do router, este será o seu canal sem fios N principal.

Standard Channel (Canal padrão) É apresentada a definição de canal padrão. Se seleccionou Wide – 40MHz Channel (Banda larga - Canal de 40MHz) para a definição Radio Band (Banda de rádio) ou Channel Width (Largura do canal) do router, o canal padrão será um canal secundário para a rede sem fios N.

Bit Rate (Velocidade de dados) É apresentada a velocidade de transmissão de dados.

Signal (Sinal) É apresentada a percentagem da potência do sinal. 100% é a potência do sinal mais forte possível; 0% é a mais fraca.

Security (Segurança) É apresentado o método de segurança da rede sem fios.

Resolução de problemas

WES610N/WET610N

O seu computador ou outro dispositivo Ethernet com fios não consegue comunicar com o router sem fios.

1. Aceda ao utilitário baseado no browser da ponte.
2. No ecrã *Basic Wireless Settings* (Definições sem fios básicas), certifique-se de que o nome da rede (SSID) corresponde ao nome da sua rede sem fios.
3. Certifique-se de que as definições de segurança (WPA, WPA2 ou WEP) correspondem às definições de segurança da sua rede sem fios.

O endereço IP da ponte necessita de ser alterado.

Se a ponte estiver ligada a uma rede com um servidor DHCP (normalmente, o router da rede), a ponte obterá o respectivo endereço IP a partir do servidor DHCP. Se não existir nenhum servidor DHCP, a ponte utilizará o respectivo endereço IP estático predefinido, **169.254.1.250**.

Se pretender que a ponte utilize sempre um endereço IP estático, siga estas instruções:

1. Aceda ao utilitário baseado no browser da ponte.
2. Clique no separador **Network Setup** (Configuração da rede).
3. No menu pendente *Network Connection Type* (Tipo de ligação da rede), seleccione **Static IP** (IP estático).
4. Preencha os campos *Static IP Address* (Endereço IP estático), *Subnet Mask* (Máscara de sub-rede) e *Default Gateway* (Gateway predefinido).
5. Clique em **Save Settings** (Guardar definições).

O computador ou outro dispositivo Ethernet com fios ligado à ponte não comunica com outro dispositivo sem fios (como um computador ou uma impressora).

Verifique o seguinte:

- Certifique-se de que o dispositivo sem fios está na mesma rede sem fios que o computador ou outro dispositivo Ethernet com fios ligado à ponte.
- Certifique-se de que está a ser utilizado o mesmo nome de rede (SSID) para todos os dispositivos na rede sem fios.
- Certifique-se de que todos os dispositivos estão na mesma rede IP e a utilizar endereços IP compatíveis.

O utilitário baseado no browser não aceita a sua palavra-passe.

Verifique o seguinte:

- A palavra-passe é sensível a maiúsculas e minúsculas. Certifique-se de que está a utilizar as letras maiúsculas e minúsculas correctas quando introduz a palavra-passe.
- Se se esqueceu da sua palavra-passe, pode repor a ponte para as respectivas predefinições de fábrica.

 Prima e mantenha premido o botão **Reset** (Repor) da ponte durante aproximadamente cinco segundos; a palavra-passe será reposta para a predefinição de fábrica, **admin**. Também serão repostas todas as outras definições da ponte para as predefinições de fábrica. (Para aceder ao utilitário baseado no browser, introduza **admin** no campo *Password* (Palavra-passe).

Depois de fazer alterações através do utilitário baseado no browser, as novas definições não são apresentadas no ecrã.

No seu browser, clique em **Refresh** (Actualizar). Se as novas definições não forem apresentadas, siga estas instruções:

1. Desligue o transformador da ponte.
2. Aguarde cinco segundos e, em seguida, ligue novamente o transformador à ponte.
3. No seu browser, clique em **Refresh** (Actualizar).

WEB
Se as suas questões não forem abordadas aqui, consulte o site da Linksys em **Linksys.com/support**

Especificações

WES610N

Modelo	WES610N
Normas	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LEDs	Alimentação, Ethernet, Wi-Fi Protected Setup™, Sem fios, ligação e actividade individual Ethernet
Portas	Ethernet (4), Alimentação
Botões	Repor, Wi-Fi Protected Setup
Tipo de cabo	CAT5e
Antenas	3 (internas)
Tipo de conector da antena	N/A
Amovíveis (Sim/Não)	Não
Modulações	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Potência RF (EIRP) em dBm	802.11a: 15 dBm (típica) @ 54Mbps 802.11b: 19 dBm (típica) @ 11 Mbps 802.11g: 16 dBm (típica) @ 54 Mbps 802.11n (2,4 GHz): 18 dBm (típica) @ MCS15 802.11n (5 GHz): 16 dBm (típica) @ MCS15
Sensibilidade de recepção	802.11a: -72 dBm (típica) @ 54 Mbps 802.11b: -85 dBm (típica) @ 11 Mbps 802.11g: -73 dBm (típica) @ 54 Mbps 802.11n (20 MHz): -75 dBm (típica) @ MCS15 802.11n (40 MHz): -69 dBm (típica) @ MCS15
Ganho da antena em dBi	1
Segurança sem fios	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bits da chave de segurança	Encriptação até 128 bits

Ambiente

Dimensões	6,97" x 5,04" x 2,68" (177 x 128 x 68 mm)
Peso	295 g
Certificação	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/rascunho n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentação	12V, 1A
Temperatura de funcionamento	32 a 104ºF (0 a 40ºC)
Temperatura de armazenamento	-4 a 140ºF (-20 a 60ºC)
Humidade de funcionamento	10 a 85%, sem condensação
Humidade de armazenamento	5 a 90%, sem condensação

As especificações estão sujeitas a alterações sem aviso prévio.

WET610N

Modelo	WET610N
Normas	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LEDs	Alimentação, Ethernet, Wi-Fi Protected Setup™, Sem fios
Portas	Ethernet, Alimentação
Botões	Repor, Wi-Fi Protected Setup
Tipo de cabo	CAT5e
Antenas	3 (internas)
Tipo de conector da antena	N/A
Amovíveis (Sim/Não)	Não
Modulações	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Potência RF (EIRP) em dBm	802.11a: 15 dBm (típica) @ 54Mbps 802.11b: 18 dBm (típica) @ 11 Mbps 802.11g: 16 dBm (típica) @ 54 Mbps 802.11n: 12 dBm (típica) @ 130 Mbps (HT20), 270 Mbps (HT40)
Sensibilidade de recepção	802.11a: -72 dBm (típica) @ 54 Mbps 802.11b: -85 dBm (típica) @ 11 Mbps 802.11g: -73 dBm (típica) @ 54 Mbps 802.11n: -70 dBm (típica) @ MCS15/2,4 GHz, -69 dBm (típica) @ MCS15/5,0 GHz
Ganho da antena em dBi	1
Segurança sem fios	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bits da chave de segurança	Encriptação até 128 bits

Ambiente

Dimensões	5,71" x 4,17" x 2,05" (145 x 106 x 52 mm)
Peso	159 g
Certificação	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/rascunho n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentação	12V, 1A
Temperatura de funcionamento	32 a 104ºF (0 a 40ºC)
Temperatura de armazenamento	-4 a 140ºF (-20 a 60ºC)
Humidade de funcionamento	10 a 85%, sem condensação
Humidade de armazenamento	5 a 90%, sem condensação

As especificações estão sujeitas a alterações sem aviso prévio.

Linksys.com/support

Cisco, o logótipo da Cisco e a Linksys são marcas comerciais ou marcas registadas da Cisco e/ou das respectivas afiliadas nos E.U.A. e noutros países.
Está disponível uma lista de marcas comerciais da Cisco em www.cisco.com/go/trademarks. Todas as outras marcas comerciais mencionadas neste documento são propriedade de seus respectivos proprietários.

© 2011 Cisco e/ou respectivas afiliadas. Todos os direitos reservados.

3425-01249



Ghidul utilizatorului

Linksys WET610N/WES610N | Punte de divertisment N pe două benzi

Cuprins

Prezentare generală a produsului

Panoul cu LED-uri 2
Panoul de porturi 3

Lista de verificări pentru securitatea fără fir

Schimbați numele sau SSID-ul implicit al rețelei fără fir 4
Schimbați parola implicită 4
Activați filtrarea adreselor MAC 4
Activați criptarea 4

Îndrumări generale pentru securitatea rețelelor 4
Sfaturi suplimentare pentru securitate 5

Configurarea avansată

Accesarea utilitarului bazat pe browser 6
Setup (Configurare) > Basic Setup (Configurare de bază) 7
Language (Limbă) 7
Network Setup (Configurare rețea) 7
Wireless (Fără fir) > Basic Wireless Settings (Setări de bază fără fir) 7
Basic Wireless Settings (Setări de bază fără fir) 8
Wireless Security (Securitate fără fir) 8
Wi-Fi Protected Setup (Configurare protejată Wi-Fi) 9
Wireless (Fără fir) > Wireless Network Site Survey (Căutare locații cu rețele fără fir) 10
Wireless Network Site Survey (Căutare locații cu rețele fără fir) 10
Wireless (Fără fir) > WMM® 11
WMM 12
Wireless (Fără fir) > Advanced Wireless Settings (Setări avansate fără fir) 13
Advanced Wireless (Avansate fără fir) 14
Administration (Administrare) > Management 14
Management 14
Administration (Administrare) > Factory Defaults (Setări implicite din fabrică) 15
Factory Defaults (Setări implicite din fabrică) 15
Administration (Administrare) > Upgrade Firmware 15
Upgrade Firmware 15
Status (Stare) > Bridge (Punte) 15
Bridge Information (Informații despre punte) 16
Local Network (Rețea locală) 16
Status (Stare) > Wireless (Fără fir). 16
Wireless (Fără fir) 16

Depanare

WES610N/WET610N 17

Specificații

WES610N 18
WET610N 19

Prezentare generală a produsului

Vă mulțumim că ați ales puntea de divertisment N pe două benzi Linksys. Puntea poate conecta orice dispozitiv Ethernet prin cablu la rețeaua dvs. fără fir. Puntea se bazează pe standardul Fără fir N pe două benzi, așadar este compatibilă cu orice router sau punct de acces fără fir N, G, A sau B. Pentru prima instalare, urmați pașii din folderul de pe CD. Pentru a configura setări avansate, utilizați utilitarul confortabil, bazat pe browser.

Panoul cu LED-uri



WES610N WET610N

Fără fir (albastru) LED-ul Fără fir se aprinde când există o conexiune fără fir. LED-ul clipește când puntea trimite sau primește date în mod activ prin rețeaua fără fir.

Butonul Wi-Fi Protected Setup (Configurare protejată Wi-Fi) Dacă routerul dvs. acceptă configurarea protejată Wi-Fi și utilizează securitate WPA sau WPA2, puteți utiliza configurarea protejată Wi-Fi pentru a conecta automat puntea. Pentru a utiliza configurarea protejată Wi-Fi, consultați „Wireless (Fără fir) > Basic Wireless Settings (Setări de bază fără fir)" de la pagina 7.

LED-ul Wi-Fi Protected Setup (Configurare protejată Wi-Fi) (albastru/portocaliu) LED-ul clipește în albastru timp de două minute în cursul configurării protejate Wi-Fi. Acesta luminează în albastru când este activată securitatea fără fir. Dacă există o eroare în cursul procesului de configurare Wi-Fi protejată, LED-ul luminează în portocaliu. Asigurați-vă că routerul rețelei acceptă configurarea protejată Wi-Fi. Așteptați până când LED-ul se stinge, apoi încercați din nou.

Ethernet (albastru) LED-ul Ethernet se aprinde când există o conexiune prin cablu. LED-ul clipește când puntea trimite sau primește date în mod activ prin porturile Ethernet.

Power (Alimentare) (albastru) LED-ul de alimentare se aprinde când puntea este alimentată.

Panoul de porturi



WES610N WET610N

Ethernet Porturile Ethernet conectează puntea la un computer sau la alt dispozitiv din rețeaua Ethernet. WES610N are patru porturi, iar WET610N are un singur port.

Reset (Resetare) Există două moduri de resetare la valorile implicite din fabrică ale punții. Fie apăsați lung butonul Reset (Resetare), timp de circa cinci secunde, fie restabiliți valorile implicite din Administration (Administrare) > Factory Defaults (Valori implicite din fabrică) în utilitarul bazat pe browser al punții. WES610N are un buton de resetare în partea de jos, iar WET610N are un buton de resetare pe panoul de porturi din spate.

Power (Alimentare) Portul de alimentare conectează puntea la adaptorul de alimentare inclus.

Lista de verificări pentru securitatea fără fir

Rețelele fără fir sunt confortabile și ușor de instalat, motiv pentru care reședințele cu acces la Internet de mare viteză le adoptă într-un ritm rapid. Deoarece rețelistica fără fir funcționează prin trimiterea informațiilor prin unde radio, poate fi mai vulnerabilă față de impostori comparativ cu o rețea tradițională, prin cablu. Ca și semnalele de la telefoanele celulare sau fără fir, și semnalele de la rețeaua dvs. fără fir pot fi interceptate. Deoarece nu puteți împiedica fizic ca cineva să se conecteze la rețeaua dvs. fără fir, trebuie să luați unele măsuri suplimentare pentru a vă păstra rețeaua securizată.

Schimbați numele sau SSID-ul implicit al rețelei fără fir

Dispozitivele fără fir au un nume sau un Service Set Identifier (SSID) implicit al rețelei fără fir, setat din fabrică. Acesta este numele rețelei dvs. fără fir și poate avea până la 32 de caractere. Produsele fără fir Linksys utilizează **linksys** ca nume implicit de rețea fără fir. Trebuie să schimbați numele rețelei fără fir într-un nume unic, pentru a deosebi rețeaua dvs. fără fir de alte rețele fără fir care pot exista în vecinătate, dar nu utilizați informații personale (precum CNP-ul), deoarece aceste informații pot fi disponibile și vizibile pentru oricine care parcurge rețelele fără fir.

Schimbați parola implicită

Pentru produsele fără fir precum punctele de acces și routerele, vi se va solicita o parolă când doriți să le modificați setările. Aceste dispozitive au o parolă implicită, setată din fabrică. Parola implicită Linksys este **admin**. Hackerii cunosc aceste valori implicite și pot încerca să le utilizeze pentru a accesa dispozitivul dvs. fără fir și a modifica setările rețelei dvs. Pentru a preveni orice modificări neautorizate, personalizați parola dispozitivului, astfel încât să fie greu de ghicit.

Activați filtrarea adreselor MAC

Routerele Linksys vă oferă posibilitatea să activați filtrarea adreselor Media Access Control (MAC). Adresa MAC este o serie unică de cifre și litere, atribuită fiecărui dispozitiv de rețea. Cu filtrarea adreselor MAC activată, accesul la rețeaua fără fir este furnizat exclusiv pentru dispozitivele fără fir cu adrese MAC specifice. De exemplu, puteți specifica adresa MAC a fiecărui computer din casă, astfel încât numai acele computere să poată accesa rețeaua dvs. fără fir.

Activați criptarea

Criptarea protejează datele transmise printr-o rețea fără fir. Wi-Fi Protected Access (Accesul Wi-Fi protejat) (WPA/WPA2) și Wired Equivalent Privacy (Confidențialitate echivalentă cu cea a unei rețele cablate) (WEP) oferă niveluri diferite de securitate pentru comunicațiile fără fir.

O rețea criptată cu WPA/WPA2 este mai securizată decât o rețea criptată cu WEP, deoarece WPA/WPA2 utilizează criptarea cu cheie dinamică. Pentru a proteja informațiile pe măsură ce acestea traversează undele aeriene, trebuie să activați cel mai înalt nivel de criptare acceptat de echipamentele dvs. de rețea.

WEP este un standard de criptare mai vechi și poate fi singura opțiune disponibilă pe anumite dispozitive mai vechi, care nu acceptă WPA.

Îndrumări generale pentru securitatea rețelelor

Securitatea rețelelor fără fir este inutilă dacă rețeaua de bază nu este securizată.

- Protejați cu parolă toate computerele din rețea și protejați cu parolă individual fișierele confidențiale.
- Schimbați parolele în mod regulat.
- Instalați software antivirus și software pentru firewall personal.
- Dezactivați partajarea de fișiere (peer-to-peer). Este posibil ca anumite aplicații să deschidă partajarea de fișiere fără consimțământul și/sau cunoștința dvs.

Sfaturi suplimentare pentru securitate

- Țineți routerele, punctele de acces sau gateway-urile fără fir departe de pereții și ferestrele exterioare.
- Opriți routerele, punctele de acces sau gateway-urile fără fir când nu sunt utilizate (pe timpul nopții, în concedii).
- Utilizați parole puternice, care au cel puțin opt caractere. Combinați litere și numere pentru a evita utilizarea cuvintelor standard, care pot fi găsite în dicționar.

Configurarea avansată

După configurarea punții urmând pașii din folderul de pe CD, puntea va fi gata de utilizare. Totuși, dacă doriți să modificați setările avansate ale acesteia, utilizați utilitarul bazat pe browser al punții. Acest capitol descrie fiecare pagină Web a utilitarului și funcțiile principale din fiecare pagină. Puteți accesa utilitarul printr-un browser Web de pe un computer conectat la punte.

Utilitarul bazat pe browser are aceste file principale: Setup (Configurare), Wireless (Fără fir), Administration (Administrare) și Status (Stare). Filele suplimentare vor fi disponibile după ce faceți clic pe una dintre filele principale.

Accesarea utilitarului bazat pe browser

Utilizați un browser Web pentru a accesa utilitarul bazat pe browser.

Dacă puntea este conectată la o rețea cu un server DHCP (de obicei routerul rețelei), puntea va obține adresa IP de la serverul DHCP. Dacă nu există niciun server DHCP, puntea va utiliza adresa IP statică implicită, **169.254.1.250**. (Dacă setați o adresă IP statică permanentă pentru punte prin intermediul utilitarului bazat pe browser, introduceți în schimb adresa IP statică.)

NOTĂ

Dacă nu cunoașteți adresa IP a punții, căutați adresa IP în tabelul de clienți DHCP al routerului dvs. (Consultați documentația pentru routerul dvs.)

Dacă nu puteți găsi adresa IP a punții, puteți reseta puntea; apăsați butonul **Reset** (Resetare) de pe punte timp de aproximativ cinci secunde, utilizând o agrafă de birou îndreptată. Astfel puntea va fi resetată la setările implicite din fabrică. Puntea va solicita o adresă IP de la serverul DHCP (de obicei routerul rețelei). Dacă nu este găsit niciun server DHCP, puntea va utiliza adresa sa IP statică implicită, **169.254.1.250**, până când detectează un server DHCP și îi este atribuită o adresă IP dinamică.

Dacă puntea nu este asociată cu un router și utilizează setările implicite din fabrică, conectați un computer la punte utilizând o conexiune Ethernet pentru a accesa utilitarul bazat pe Web. Va trebui să configurați conexiunea Ethernet de pe computer cu o adresă IP statică și o mască de subrețea.

Adresa IP a adaptorului dvs. Ethernet trebuie să fie setată la o adresă IP specifică.

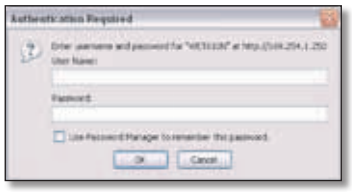
1. În câmpul *Adresă IP*, introduceți **169.254.x.y** (x trebuie înlocuit cu un număr între 1 și 254, iar y trebuie înlocuit cu un număr între 0 și 255).
2. În câmpul *Mască subrețea*, introduceți **255.255.0.0**.

NOTĂ

Pașii pentru atribuirea unei adrese IP statice adaptorului Ethernet de pe computerul dvs. variază în funcție de sistemul de operare. Pentru instrucțiuni, consultați documentația de ajutor a sistemului dvs. de operare specific.

După ce ați atribuit adaptorului dvs. Ethernet o adresă IP statică, lansați browserul Web și introduceți adresa IP a adaptorului IP (setarea implicită este **169.254.1.250**) în câmpul *Adresă*. Apăsați **Enter**.

Apare un ecran prin care se solicită parola. (Utilizatorii altor sisteme de operare decât Windows XP vor vedea un ecran similar.) Lăsați necompletat câmpul *Nume de utilizator*. Introduceți parola pe care ați creat-o în cursul Expertului de instalare. Dacă nu ați creat o parolă nouă, utilizați parola implicită, **admin**. (Puteți seta o parolă nouă în ecranul *Administration* (Administrare) > *Management*.) Faceți clic pe **OK** pentru a continua.



NOTĂ

Dacă nu apare ecranul prin care vi se solicită parola, așteptați două minute și încercați din nou.

Setup (Configurare) > Basic Setup (Configurare de bază)

Primul ecran care apare este ecranul *Basic Setup* (Configurare de bază). Utilizați acest ecran pentru a schimba limba utilitarului bazat pe browser sau pentru a modifica setările rețelei Ethernet conectate prin cablu la punte.





Language (Limbă)

Language (Limbă) Această setare este utilizată pentru a seta limba afișată de utilitarul bazat pe browser. Selectați limba dorită din meniul derulant.

Network Setup (Configurare rețea)

Această secțiune stabilește dacă adresa IP a punții este obținută automat de la un server DHCP, precum routerul rețelei dvs. (Automatic Configuration (Configurare automată) - DHCP) sau este setată manual (Static IP (IP static)).

Bridge IP (IP punte) Dacă rețeaua dvs. are un server DHCP, precum routerul rețelei dvs., care atribuie adrese IP dispozitivelor din rețea, păstrați setarea implicită, **Automatic Configuration** (Configurare automată) **- DHCP**. Puntea va solicita o adresă IP de la serverul DHCP (de obicei routerul rețelei). Dacă nu este găsit niciun server DHCP, puntea va utiliza adresa sa IP statică implicită, **169.254.1.250**, până când detectează un server DHCP și îi este atribuită o adresă IP dinamică.

Dacă doriți să setați o adresă IP statică permanentă pentru punte, selectați **Static IP** (IP static).

Dacă selectați Static IP (IP static), completați următoarele câmpuri:

- **Static IP Address** (Adresă IP statică) Introduceți o adresă IP unică, care va fi utilizată pentru accesarea utilitarului bazat pe browser.
- **Subnet Mask** (Mască subrețea) Introduceți masca de subrețea a rețelei dvs. prin cablu.
- **Default Gateway** (Gateway implicit) Introduceți adresa IP a gateway-ului implicit pentru rețeaua dvs. (în majoritatea cazurilor, acesta este routerul dvs.).

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Wireless (Fără fir) > Basic Wireless Settings (Setări de bază fără fir)

Utilizați ecranul *Basic Wireless Settings* (Setări de bază fără fir) pentru a configura setările de bază fără fir și setările de securitate ale punții.

Există două moduri de a configura setările punții, manual și configurare protejată Wi-Fi. Configurarea protejată Wi-Fi este o caracteristică ce facilitează configurarea rețelei dvs. fără fir. Dacă routerul rețelei dvs. acceptă configurarea protejată Wi-Fi și utilizează securitate WPA sau WPA2, puteți utiliza configurarea protejată Wi-Fi pentru a conecta automat puntea.

Configuration View (Vizualizare configurare) Pentru a configura manual rețeaua fără fir, selectați **Manual**. Consultați **Basic Wireless Settings** (Setări de bază fără fir), **pagina 8**. Pentru a utiliza configurarea protejată Wi-Fi, selectați **Wi-Fi Protected Setup** (Configurare protejată Wi-Fi). Consultați **Wi-Fi Protected Setup (Configurare protejată Wi-Fi)**, **pagina 9**.

Basic Wireless Settings (Setări de bază fără fir)



Network Name (SSID) (Nume rețea (SSID) SSID-ul este numele de rețea partajat de toate punctele dintr-o rețea fără fir. SSID trebuie să fie identic pentru toate dispozitivele din rețeaua fără fir. Acesta face distincția dintre majuscule și minuscule și nu trebuie să depășească 32 de caractere (utilizați orice caractere de la tastatură). Asigurați-vă că această setare corespunde setării de pe routerul sau punctul dvs. de acces fără fir. Pentru securitate suplimentară, trebuie să schimbați SSID-ul implicit (**linksys**) la un nume unic.

Wireless Security (Securitate fără fir)

Puntea acceptă următoarele opțiuni de securitate fără fir: WPA Personal, WPA2 Personal și WEP. WPA (Wi-Fi Protected Access - Acces protejat Wi-Fi) și WPA2 sunt metode de securitate mai puternice decât WEP (Wired Equivalent Privacy - Confidențialitate echivalentă cu cea a unei rețele cablate). Pentru mai multe informații despre securitatea fără fir, consultați "Lista de verificări pentru securitatea fără fir", pagina 4.

Security Mode (Mod de securitate)

Selectați metoda de securitate pentru rețeaua dvs. fără fir. Dacă nu doriți să utilizați securitatea fără fir, păstrați valoarea implicită, **Disabled** (Dezactivat).

NOTĂ
Rețineți că fiecare dispozitiv din rețeaua dvs. fără fir TREBUIE să utilizeze aceeași metodă de securitate și parolă/cheie, altfel dispozitivele fără fir nu vor putea să comunice unele cu altele.

WPA Personal

WPA este un standard de securitate mai strict decât criptarea WEP.



Encryption (Criptare) WPA acceptă metoda de criptare TKIP, cu chei de criptare dinamice.

Passphrase (Parolă) Introduceți cheia partajată de punte și de routerul sau punctul dvs. de acces fără fir. Aceasta trebuie să aibă 8-63 caractere.

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

WPA2 Personal

WPA2 este o versiune mai avansată și mai securizată a WPA.



Encryption (Criptare) WPA2 acceptă două metode de criptare, TKIP și AES, cu chei de criptare dinamice. Selectați metoda de criptare, **AES** ori **TKIP or AES** (TKIP sau AES). Selecția implicită este **AES**.

Passphrase (Parolă) Introduceți cheia partajată de punte și de routerul sau punctul de acces fără fir. Aceasta trebuie să aibă 8-63 caractere.

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

WEP

WEP este o metodă de criptare de bază, care nu este la fel de sigură ca WPA sau WPA2.



Encryption (Criptare) Selectați un nivel de criptare WEP, **40/64 bits (10 hex digits)** (40/64 de biți (10 cifre hexazecimale) sau **104/128 bits (26 hex digits)** (104/128 biți (26 de cifre hexazecimale). Valoarea implicită este **40/64 bits (10 hex digits)** (40/64 de biți (10 cifre hexazecimale).

Key 1 (Cheie 1) Introduceți cheia WEP a rețelei dvs.

Tx Key (Cheie de transmisie) **Cheia 1** este cheia de transmisie utilizată de punte.

Authentication (Autentificare) Valoarea implicită este **Auto** (Automat), care permite utilizarea autentificării în sistem Open (Deschis) sau Shared key (Cheie partajată). Selectați **Open** (Deschis) pentru a utiliza autentificarea în sistem deschis; expeditorul și destinatarul nu utilizează o cheie WEP pentru autentificare. Selectați **Shared** (Partajat) pentru a utiliza autentificarea cu cheie partajată; expeditorul și destinatarul utilizează o cheie WEP pentru autentificare.

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Wi-Fi Protected Setup (Configurare protejată Wi-Fi)

Sunt disponibile două metode. Utilizați metoda care se aplică routerului pe care-l utilizați.





Metoda nr. 1

Utilizați această metodă dacă routerul dvs. deține un buton Wi-Fi Protected Setup (Configurare protejată Wi-Fi).

1. Faceți clic sau apăsați pe butonul **Wi-Fi Protected Setup** (Configurare protejată Wi-Fi) de pe router.
2. În decurs de două minute, faceți clic pe butonul **Wi-Fi Protected Setup** (Configurare protejată Wi-Fi) din ecranul *Wi-Fi Protected Setup* (Configurare protejată Wi-Fi) al punții.
3. După ce puntea a fost configurată, faceți clic pe **Close** (Închidere).

Ecranul *Wi-Fi Protected Setup* (Configurare protejată Wi-Fi) afișează Link Status (Stare legătură), Network Name (SSID) (Nume rețea (SSID)) și Security method (Metodă de securitate).

Metoda nr. 2

Utilizați această metodă dacă routerul dvs. solicită numărul PIN al punții.

1. În ecranul *Wi-Fi Protected Setup* (Configurare protejată Wi-Fi) **al routerului**, introduceți numărul PIN din ecranul *Wi-Fi Protected Setup* (Configurare protejată Wi-Fi) al **punții**. Apoi faceți clic pe **Register** (Înregistrare) sau pe butonul corespunzător. (Acesta este indicat și pe eticheta din partea de jos a punții.)
2. În ecranul *Wi-Fi Protected Setup* (Configurare protejată Wi-Fi) al **punții**, faceți clic pe **OK**.
3. După ce puntea a fost configurată, faceți clic pe **Close** (Închidere).

Ecranul *Wi-Fi Protected Setup* (Configurare protejată Wi-Fi) afișează Link Status (Stare legătură), Network Name (SSID) (Nume rețea (SSID)) și Security method (Metodă de securitate).

Wireless (Fără fir) > Wireless Network Site Survey (Căutare locații cu rețele fără fir)

Faceți clic pe fila **Wireless Network Site Survey** (Căutare locații cu rețele fără fir) pentru a începe o căutare de locații. Ecranul *Wireless Network Site Survey* (Căutare locații cu rețele fără fir) enumeră rețelele fără fir detectate de punte.



Wireless Network Site Survey (Căutare locații cu rețele fără fir)

Number of Wireless Networks (Număr de rețele fără fir) Este afișat numărul de rețele fără fir detectate de punte.

Select (Selectare) Pentru a vă conecta la o rețea fără fir, faceți clic pe **Select** (Selectare). Apoi faceți clic pe **Connect** (Conectare).

Wireless Network Name (Nume rețea fără fir) Numele sau SSID-ul rețelei pentru rețeaua fără fir afișată.

GHz Este afișată banda radio a rețelei fără fir.

Signal (Semnal) Este afișat procentajul de intensitate a semnalului. 100% este cel mai ridicat nivel de intensitate a semnalului posibil; 0% este cel mai redus nivel posibil.

Security (Securitate) Dacă rețeaua acceptă configurarea protejată Wi-Fi, este afișată pictograma de configurare protejată Wi-Fi . Este afișată metoda de securitate utilizată de rețeaua fără fir.

Faceți clic pe **Refresh** (Reîmprospătare) pentru a actualiza informațiile de pe ecran.

După ce ați selectat o rețea, faceți clic pe **Connect** (Conectare). Apare un ecran nou. Urmați instrucțiunile pentru metoda de securitate a rețelei dvs.

WPA



Network Name (SSID) (Nume rețea (SSID)) Numele rețelei selectate este afișat automat.

Security Mode (Mod de securitate) WPA Personal este afișat automat.

Encryption (Criptare) WPA acceptă metoda de criptare TKIP, cu chei de criptare dinamice.

Passphrase (Parolă) Introduceți cheia partajată de punte și de routerul sau punctul de acces fără fir. Aceasta trebuie să aibă 8-63 caractere.

Faceți clic pe **Refresh** (Reîmprospătare) pentru a actualiza informațiile de pe ecran.

După ce ați introdus setările de securitate, faceți clic pe **Connect** (Conectare).

WPA2



Network Name (SSID) (Nume rețea (SSID)) Numele rețelei selectate este afișat automat.

Security Mode (Mod de securitate) WPA2 Personal este afișat automat.

Encryption (Criptare) WPA2 acceptă două metode de criptare, TKIP și AES, cu chei de criptare dinamice. Selectați metoda de criptare, **AES** ori **TKIP or AES** (TKIP sau AES).

Passphrase (Parolă) Introduceți cheia partajată de punte și de routerul sau punctul de acces fără fir. Aceasta trebuie să aibă 8-63 caractere.

Faceți clic pe **Refresh** (Reîmprospătare) pentru a actualiza informațiile de pe ecran.

După ce ați introdus setările de securitate, faceți clic pe **Connect** (Conectare).

WEP



Network Name (SSID) (Nume rețea (SSID)) Numele rețelei selectate este afișat automat.

Security Mode (Mod de securitate) WEP este afișat automat.

Encryption (Criptare) Selectați un nivel de criptare WEP, **40/64 de biți (10 hex digits)** (40/64 de biți (10 cifre hexazecimale)) sau **104/128 de biți (26 hex digits)** (104/128 de biți (26 cifre hexazecimale)).

Key 1 (Cheie 1) Introduceți cheia WEP a rețelei dvs.

Tx Key (Cheie de transmisie) **Cheia 1** este cheia de transmisie utilizată de punte.

Authentication (Autentificare) Valoarea implicită este **Auto** (Automat), care permite utilizarea autentificării în sistem Open (Deschis) sau Shared key (Cheie partajată). Selectați **Open** (Deschis) pentru a utiliza autentificarea în sistem deschis; expeditorul și destinatarul nu utilizează o cheie WEP pentru autentificare. Selectați **Shared** (Partajat) pentru a utiliza autentificarea cu cheie partajată; expeditorul și destinatarul utilizează o cheie WEP pentru autentificare.

Faceți clic pe **Refresh** (Reîmprospătare) pentru a actualiza informațiile de pe ecran.

După ce ați introdus setările de securitate, faceți clic pe **Connect** (Conectare).

Wireless (Fără fir) > WMM®

Configurați setările Wireless MultiMedia (WMM). WMM prioritizează pachetele în funcție de modul lor de acces (tipul de trafic): Background (În fundal), Best Effort (Cel mai performant), Video sau Voice (Voce). Aceste setări trebuie reglate numai de un administrator expert, deoarece setările incorecte pot reduce performanța fără fir.



NOTĂ
Setările din ecranul *WMM* sunt proiectate numai pentru utilizatorii avansați.

WMM

Access Mode (Mod de acces)

Puteți atribui setări diferite celor patru moduri de acces disponibile. Selectați modul pe care doriți să-l configurați: **Background** (În fundal), **Best Effort** (Cel mai performant), **Video** sau **Voice** (Voce). Urmați instrucțiunile pentru modul pe care-l selectați.

Background (În fundal)

Use Aggregation (Utilizare agregare) Această opțiune definește dacă stratul Media Access Control (MAC) va configura sau nu o sesiune Add Block Acknowledgement (ADDBA). Valoarea implicită este **No** (Nu). Selectați **Yes** (Da) pentru a activa această opțiune.

Accept Aggregation (Acceptare agregare) Această opțiune definește dacă stratul MAC va accepta sau nu o cerere ADDBA. Valoarea implicită este **Yes** (Da). Selectați **No** (Nu) pentru a dezactiva această opțiune.

Max. Number of Packets in Aggregation (Număr max. de pachete din agregare) Această opțiune definește numărul maxim de pachete (subcadre) din agregare. Intervalul este **0** - **7**. Valoarea implicită este **7**.

Max. Aggregation Size (Dimensiune max. agregare) Această opțiune definește dimensiunea maximă a agregării (în bytes). Intervalul este **0** - **16000**. Valoarea implicită este **12000**.

Timeout Internal (Interval expirare) Această opțiune definește perioada de expirare în care agregarea trebuie închisă cu o „condiție de închidere" înainte de a fi închisă de cronometru. Intervalul este **0** - **100** ms. Valoarea implicită este **3**.

Min. Size of Packet in Aggregation (Dimensiune min. a pachetului din agregare) Această opțiune definește dimensiunea minimă (în bytes) a pachetelor de cumulat în agregare. Intervalul este **0** - **1500**. Valoarea implicită este **10**.

ADDBA Timeout (Expirare ADDBA) Această opțiune definește durata după care este întreruptă configurarea ADDBA, dacă nu există schimburi de cadre în decursul acestei durate, prin intermediul convenției Block Acknowledgement (ACK). Intervalul este **0** - **65535** ms. Valoarea implicită este **0**, care dezactivează expirarea.

Aggregation Window Size (Dimensiune fereastră de agregare) Această opțiune definește numărul maxim de pachete transmise fără a obține ACK. Intervalul este **0** - **64**. Valoarea implicită este **64**.

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Best Effort (Cel mai performant)

Use Aggregation (Utilizare agregare) Această opțiune definește dacă stratul Media Access Control (MAC) va configura sau nu o sesiune Add Block Acknowledgement (ADDBA). Valoarea implicită este **Yes** (Da). Selectați **No** (Nu) pentru a dezactiva această opțiune.

Accept Aggregation (Acceptare agregare) Această opțiune definește dacă stratul MAC va accepta sau nu o cerere ADDBA. Valoarea implicită este **Yes** (Da). Selectați **No** (Nu) pentru a dezactiva această opțiune.

Max. Number of Packets in Aggregation (Număr max. de pachete din agregare) Această opțiune definește numărul maxim de pachete (subcadre) din agregare. Intervalul este **0** - **10**. Valoarea implicită este **10**.

Max. Aggregation Size (Dimensiune max. agregare) Această opțiune definește dimensiunea maximă a agregării (în bytes). Intervalul este **0** - **20000**. Valoarea implicită este **16000**.

Timeout Internal (Interval expirare) Această opțiune definește perioada de expirare în care agregarea trebuie închisă cu o „condiție de închidere" înainte de a fi închisă de cronometru. Intervalul este **0** - **100** ms. Valoarea implicită este **3**.

Min. Size of Packet in Aggregation (Dimensiune min. a pachetului din agregare) Această opțiune definește dimensiunea minimă (în bytes) a pachetelor de cumulat în agregare. Intervalul este **0** - **1500**. Valoarea implicită este **10**.

ADDBA Timeout (Expirare ADDBA) Această opțiune definește durata după care este întreruptă configurarea ADDBA, dacă nu există schimburi de cadre în decursul acestei durate, prin intermediul convenției Block Acknowledgement (ACK). Intervalul este **0** - **65535** ms. Valoarea implicită este **0**, care dezactivează expirarea.

Aggregation Window Size (Dimensiune fereastră de agregare) Această opțiune definește numărul maxim de pachete transmise fără a obține ACK. Intervalul este **0** - **64**. Valoarea implicită este **64**.

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Video

Use Aggregation (Utilizare agregare) Această opțiune definește dacă stratul Media Access Control (MAC) va configura sau nu o sesiune Add Block Acknowledgement (ADDBA). Valoarea implicită este **Yes** (Da). Selectați **No** (Nu) pentru a dezactiva această opțiune.

Accept Aggregation (Acceptare agregare) Această opțiune definește dacă stratul MAC va accepta sau nu o cerere ADDBA. Valoarea implicită este **Yes** (Da). Selectați **No** (Nu) pentru a dezactiva această opțiune.

Max. Number of Packets in Aggregation (Număr max. de pachete din agregare) Această opțiune definește numărul maxim de pachete (subcadre) din agregare. Intervalul este **0** - **7**. Valoarea implicită este **7**.

Max. Aggregation Size (Dimensiune max. agregare) Această opțiune definește dimensiunea maximă a agregării (în bytes). Intervalul este **0** - **16000**. Valoarea implicită este **12000**.

Timeout Internal (Interval expirare) Această opțiune definește perioada de expirare în care agregarea trebuie închisă cu o „condiție de închidere" înainte de a fi închisă de cronometru. Intervalul este **0** - **100** ms. Valoarea implicită este **3**.

Min. Size of Packet in Aggregation (Dimensiune min. a pachetului din agregare) Această opțiune definește dimensiunea minimă (în bytes) a pachetelor de cumulat în agregare. Intervalul este **0** - **1500**. Valoarea implicită este **10**.

ADDBA Timeout (Expirare ADDBA) Această opțiune definește durata după care este întreruptă configurarea ADDBA, dacă nu există schimburi de cadre în decursul acestei durate, prin intermediul convenției Block Acknowledgement (ACK). Intervalul este **0** - **65535** ms. Valoarea implicită este **0**, care dezactivează expirarea.

Aggregation Window Size (Dimensiune fereastră de agregare) Această opțiune definește numărul maxim de pachete transmise fără a obține ACK. Intervalul este **0** - **64**. Valoarea implicită este **64**.

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Voice (Voce)

Use Aggregation (Utilizare agregare) Această opțiune definește dacă stratul Media Access Control (MAC) va configura sau nu o sesiune Add Block Acknowledgement (ADDBA). Valoarea implicită este **Yes** (Da). Selectați **No** (Nu) pentru a dezactiva această opțiune.

Accept Aggregation (Acceptare agregare) Această opțiune definește dacă stratul MAC va accepta sau nu o cerere ADDBA. Valoarea implicită este **Yes** (Da). Selectați **No** (Nu) pentru a dezactiva această opțiune.

Max. Number of Packets in Aggregation (Număr max. de pachete din agregare) Această opțiune definește numărul maxim de pachete (subcadre) din agregare. Intervalul este **0** - **2**. Valoarea implicită este **2**.

Max. Aggregation Size (Dimensiune max. agregare) Această opțiune definește dimensiunea maximă a agregării (în bytes). Intervalul este **0** - **16000**. Valoarea implicită este **10000**.

Timeout Internal (Interval expirare) Această opțiune definește perioada de expirare în care agregarea trebuie închisă cu o „condiție de închidere" înainte de a fi închisă de cronometru. Intervalul este **0** - **100** ms. Valoarea implicită este **10**.

Min. Size of Packet in Aggregation (Dimensiune min. a pachetului din agregare) Această opțiune definește dimensiunea minimă (în bytes) a pachetelor de cumulat în agregare. Intervalul este **0** - **1500**. Valoarea implicită este **10**.

ADDBA Timeout (Expirare ADDBA) Această opțiune definește durata după care este întreruptă configurarea ADDBA, dacă nu există schimburi de cadre în decursul acestei durate, prin intermediul convenției Block Acknowledgement (ACK). Intervalul este **0** - **65535** ms. Valoarea implicită este **0**, care dezactivează expirarea.

Aggregation Window Size (Dimensiune fereastră de agregare) Această opțiune definește numărul maxim de pachete transmise fără a obține ACK. Intervalul este **0** - **64**. Valoarea implicită este **64**.

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Wireless (Fără fir) > Advanced Wireless Settings (Setări avansate fără fir)

Configurați setările avansate fără fir ale punții. Aceste setări trebuie reglate numai de un administrator expert, deoarece setările incorecte pot reduce performanța fără fir.



NOTĂ
Setările din ecranul *Advanced Wireless Settings* (Setări avansate fără fir) sunt proiectate numai pentru utilizatorii avansați.

Advanced Wireless (Avansate fără fir)

Use LDPC (Utilizare LDPC) Low-Density Parity-Check Code (LDPC) activează sau dezactivează corectarea erorilor pentru a reduce probabilitatea de pierdere a datelor în canalele cu interferențe. Algoritmul de adaptare a ratei a dezactivat automat codarea LDPC dacă funcționează la rate PHY mari (mai mari de 162). Pentru a utiliza schema avansată de corectare a erorilor LDCP, păstrați valoarea implicită, **Yes** (Da). În caz contrar, selectați **No** (Nu).

ERP Protection Type (Tip protecție ERP) Această opțiune configurează protecția pachetelor OFDM în ciuda prezenței stațiilor 802.11b în cadrul rețelei fără fir. Trimițând pachete RTS/CTS sau CTS2Self la rate 802.11b, puntea informează rețeaua fără fir că urmează să fie transferate pachete OFDM și protejează pachetele din rețeaua fără fir. Pachetele RTS/CTS și CTS2Self creează suprasolicitare, care poate duce la rate de transfer mai mici.

Opțiunea RTS/CTS oferă acoperire mai bună, dar rate de transfer mai reduse comparativ cu CTS2Self, deoarece opțiunea RTS/CTS include confirmarea de la dispozitivul destinatar. Pentru a utiliza opțiunea RTS/CTS, păstrați valoarea implicită, **RTS/CTS**. Opțiunea None (Niciunul) poate produce coliziuni între pachetele OFDM și CCK. Pentru a utiliza opțiunea None (Niciunul), selectați **None** (Niciunul). Pentru a utiliza opțiunea CTS2Self, selectați **CTS2Self**.

11n Protection Type (Tip protecție 11n) Această opțiune configurează protecția de la dispozitivele fără rată High Throughput (HT) din rețeaua fără fir. În cazul în care routerul (sau punctul de acces) fără fir detectează o asociere a unui dispozitiv moștenit fără HT, va semnala tuturor dispozitivelor HT să utilizeze mecanisme RTS/CTS sau CTS2Self înainte de fiecare transmisie de date. Această caracteristică acceptă și toate protecțiile standard 802.11n, inclusiv MIMO.

Opțiunea RTS/CTS oferă acoperire mai bună, dar rate de transfer mai reduse comparativ cu CTS2Self, deoarece opțiunea RTS/CTS include confirmarea de la dispozitivul destinatar. Pentru a utiliza opțiunea RTS/CTS, păstrați valoarea implicită, **RTS/CTS**. Opțiunea None (Niciunul) poate produce coliziuni între pachetele HT și cel moștenite. Pentru a utiliza opțiunea None (Niciunul), selectați **None** (Niciunul). Pentru a utiliza opțiunea CTS2Self, selectați **CTS2Self**.

Percentage of maximal transmit power (Procentaj putere de transmisie maximală) Această opțiune setează procentajul de putere de transmisie maximală relativ la restricțiile de domenii de reglementare. De exemplu, dacă restricția de domenii de reglementare permite transmisii de până la 20 dB, setarea procentajului la 50% permite o putere de transmisie maximală de 10 dB. Selectați procentajul pe care doriți să-l utilizați: **12%**, **25%**, **50%** sau **100%**. Valoarea implicită este **100%**.

QoS Classification Type (Tip clasificare QoS) Această opțiune setează maparea 802.1D sau 802.1Q din câmpul IP DSCP/TOS la prioritățile WMM (Background (În fundal), Best Effects (Cel mai performant), Video, Voice (Voce)). Păstrați valoarea implicită, **802.1D**, sau selectați **802.1Q**, care este utilizată de anumite fluxuri IPTV.

Re-establish Ethernet connection when initiating wireless connection (Restabilire conexiune Ethernet la inițierea conexiunii fără fir) Pentru a declanșa descoperirea DHCP de la dispozitivul care rezidă în spatele punții, puntea va reseta legătura Ethernet dintre punte și dispozitiv de fiecare dată când este stabilită o conexiune fără fir. Pentru a dezactiva acest comportament, selectați **No** (Nu). În caz contrar, păstrați valoarea implicită, **Yes** (Da).

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Administration (Administrare) > Management

Utilizați acest ecran pentru a gestiona anumite funcții ale punții: accesați utilitarul bazat pe Web, efectuați o copie de siguranță a fișierului de configurare și reinițializați.



Management

Bridge Access (Acces punte)

Utilizați o parolă pentru a proteja accesul la utilitarul bazat pe browser.

Bridge Password (Parolă punte) Introduceți o parolă nouă pentru punte.

Re-enter to confirm (Reintroducere pentru confirmare) Introduceți parola din nou pentru a o confirma.

Idle Timeout (Expirare la inactivitate) Conectarea expiră după o perioadă de inactivitate pe care o specificați. Intervalul este **60** - **3600** secunde. Valoarea implicită este **600**.

Web Access (Acces Web)

Access via Wireless (Acces fără fir) Dacă utilizați puntea într-un domeniu public, unde acordați acces fără fir invitaților, puteți dezactiva accesul fără fir la utilitarul bazat pe browser al punții. Veți putea accesa utilitarul bazat pe browser numai printr-o conexiune prin cablu dacă dezactivați setarea. Păstrați valoarea implicită, **Enabled** (Activat), pentru a permite accesul fără fir la utilitarul bazat pe browser al punții sau selectați **Disabled** (Dezactivat) pentru a bloca accesul fără fir la utilitar.

Backup and Restore (Copiere de siguranță și restabilire)

Backup (Copiere de siguranță) Pentru a crea o copie de siguranță a fișierului de configurare al punții, faceți clic pe **Backup Configurations** (Copiere de siguranță configurații). Apoi urmați instrucțiunile de pe ecran.

Restore (Restabilire) Faceți clic pe **Browse** (Parcurgere) și selectați fișierul de configurare. Apoi faceți clic pe **Restore Configurations** (Restabilire configurații).

System Reboot (Reinițializare sistem)

Reboot (Reinițializare) Pentru a reinițializa sau a reporni puntea, faceți clic pe **Start to Reboot** (Pornire reinițializare).

Faceți clic pe **Save Settings** (Salvare setări) pentru a aplica modificările sau faceți clic pe **Cancel Changes** (Anulare modificări) pentru a anula modificările.

Administration (Administrare) > Factory Defaults (Setări implicite din fabrică)

Utilizați acest ecran pentru a restabili configurația punții la setările implicite din fabrică.

Factory Defaults (Setări implicite din fabrică)

Restore All Settings (Restabilire toate setările) Pentru a reseta setările punții la valorile implicite din fabrică, faceți clic pe **Restore All Settings** (Restabilire toate setările). Toate setările pe care le-ați salvat se vor pierde atunci când sunt restabilite setările implicite.



Administration (Administrare) > Upgrade Firmware

Utilizați acest ecran pentru a efectua upgrade-ul firmware-ului punții. Nu efectuați upgrade-ul firmware-ului decât dacă aveți probleme cu puntea sau dacă noul firmware are o caracteristică pe care doriți s-o utilizați.



Înainte de a efectua upgrade-ul firmware-ului, descărcați fișierul de upgrade al firmware-ului punții de pe site-ul Web Linksys, **www.Linksys.com/support**.

Upgrade Firmware

Please select a file to upgrade (Selectați un fișier pentru upgrade) Faceți clic pe **Browse** (Parcurgere) și selectați fișierul pentru upgrade-ul firmware-ului. Apoi faceți clic pe **Start to Upgrade** (Pornire upgrade) și urmați instrucțiunile de pe ecran.

Status (Stare) > Bridge (Punte)

Sunt afișate informații despre starea curentă a punții.



Bridge Information (Informații despre punte)

Firmware Version (Versiune firmware) Este afișat firmware-ul curent al punții.

Local Network (Rețea locală)

Local MAC Address (Adresă MAC locală) Este afișată adresa MAC a punții, așa cum este văzută în rețeaua dvs. Ethernet locală.

IP Address (Adresă IP) Este afișată adresa IP a punții, așa cum este văzută în rețeaua dvs. Ethernet locală.

Subnet Mask (Mască subrețea) Este afișată masca de subrețea configurată pentru rețeaua dvs. locală.

Status (Stare) > Wireless (Fără fir)

Sunt afișate informații despre rețeaua dvs. fără fir.



Wireless (Fără fir)

Link Status (Stare legătură) Este afișată starea conexiunii la rețeaua dvs. fără fir.

MAC Address (Adresă MAC) Este afișată adresa MAC a punții, așa cum este văzută în rețeaua dvs. fără fir locală.

Network Name (SSID) (Nume rețea (SSID) Este afișat numele sau SSID-ul rețelei fără fir.

BSSID Este afișată adresa MAC fără fir a routerului (sau punctului de acces) fără fir conectat.

Radio Band (Bandă radio) Este afișată banda radio a rețelei fără fir.

Channel Width (Lățime canal) Este afișată lățimea canalului, în MHz, utilizată de rețeaua dvs. fără fir.

Wide Channel (Canal lat) În funcție de setările de canale ale routerului rețelei dvs., este afișat Wide Channel (Canal lat). Dacă ați selectat Wide - 40MHz Channel (Canal lat - 40 MHz) pentru setarea Radio Band (Bandă radio) sau Channel Width (Lățime canal) a routerului, acesta va fi principalul dvs. canal fără fir N.

Standard Channel (Canal standard) Este afișată setarea Standard Channel (Canal standard). Dacă ați selectat Wide - 40MHz Channel (Canal lat - 40 MHz) pentru setarea Radio Band (Bandă radio) sau Channel Width (Lățime canal) a routerului, acesta va fi canalul dvs. fără fir N secundar.

Bit Rate (Rată de biți) Este afișată rata de transmisie a datelor.

Signal (Semnal) Este afișat procentajul de intensitate a semnalului. 100% este cel mai ridicat nivel de intensitate a semnalului posibil; 0% este cel mai redus nivel posibil.

Security (Securitate) Este afișată metoda de securitate a rețelei dvs. fără fir.

Depanare

WES610N/WET610N

Computerul dvs. sau al dispozitiv Ethernet cablat nu poate comunica cu routerul fără fir.

1. Accesați utilitarul bazat pe browser al punții.
2. În ecranul *Basic Wireless Settings* (Setări de bază fără fir), asigurați-vă că numele rețelei (SSID-ul) corespunde cu numele rețelei dvs. fără fir.
3. Asigurați-vă că setările de securitate (WPA, WPA2 sau WEP) corespund cu setările de securitate ale rețelei dvs. fără fir.

Adresa IP a punții trebuie schimbată.

Dacă puntea este conectată la o rețea cu un server DHCP (de obicei routerul rețelei), puntea va obține adresa IP de la serverul DHCP. Dacă nu există niciun server DHCP, puntea va utiliza adresa IP statică implicită, **169.254.1.250**.

Dacă doriți ca puntea să utilizeze întotdeauna o adresă IP statică, urmați aceste instrucțiuni:

1. Accesați utilitarul bazat pe browser al punții.
2. Faceți clic pe fila **Network Setup** (Configurare rețea).
3. Din meniul derulant *Network Connection Type* (Tip conexiune rețea), selectați **Static IP** (IP static).
4. Completați câmpurile *Static IP Address* (Adresă IP statică), *Subnet Mask* (Mască subrețea) și *Default Gateway* (Gateway implicit).
5. Faceți clic pe **Save Settings** (Salvare setări).

Computerul sau alt dispozitiv Ethernet cablat compatibil cu puntea nu comunică cu alt dispozitiv compatibil cu tehnologia fără fir (precum un computer sau o imprimantă).

Verificați următoarele:

- Asigurați-vă că dispozitivul compatibil cu tehnologia fără fir este în aceeași rețea fără fir ca și computerul sau alt dispozitiv Ethernet cablat conectat la punte.
- Asigurați-vă că pentru toate dispozitivele din rețeaua fără fir este utilizat același nume de rețea (SSID).
- Asigurați-vă că toate dispozitivele sunt în aceeași rețea IP, care utilizează adrese IP compatibile.

Utilitarul bazat pe browser nu acceptă parola dvs.

Verificați următoarele:

- Parola ține cont de majuscule și minuscule. Asigurați-vă că utilizați tastatura corect când introduceți parola.
- Dacă uitați parola, puteți reseta puntea la valorile sale implicite din fabrică.

 Apăsați lung butonul **Reset** (Resetare) al punții, timp de circa cinci secunde; parola va fi resetată la valoarea sa implicită din fabrică, **admin**. În același timp, toate celelalte setări ale punții vor fi resetate la valorile implicite din fabrică. (Pentru a accesa utilitarul bazat pe browser, introduceți **admin** în câmpul *Password* (Parolă).)

După ce efectuați modificările prin intermediul utilitarului bazat pe browser, noile setări nu sunt afișate pe ecran.

În browserul dvs. Web, faceți clic pe **Refresh** (Reîmprospătare). Dacă noile setări nu sunt afișate, urmați aceste instrucțiuni:

1. Deconectați adaptorul de alimentare de la punte.
2. Așteptați cinci secunde, apoi reconectați adaptorul de alimentare la punte.
3. În browserul dvs. Web, faceți clic pe **Refresh** (Reîmprospătare).

WEB
Dacă întrebările dvs. nu sunt adresate aici, consultați site-ul Web Linksys, la adresa **Linksys.com/support**

Specificații

WES610N

Model	WES610N
Standarde	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED-uri	Alimentare, Ethernet, Wi-Fi Protected Setup™, Fără fir, legătură și activitate Ethernet individuală
Porturi	Ethernet (4), Alimentare
Butoane	Resetare, Wi-Fi Protected Setup
Tip de cablaj	CAT5e
Antene	3 (interne)
Tip de conector la antenă	N/A
Detașabil (Da/Nu)	Nu
Modulații	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Putere RF (EIRP) în dBm	802.11a: 15 dBm (tipic) la 54 Mb/s 802.11b: 19 dBm (tipic) la 11 Mb/s 802.11g: 16 dBm (tipic) la 54 Mb/s 802.11n (2,4 GHz): 18 dBm (tipic) la MCS15 802.11n (5 GHz): 16 dBm (tipic) la MCS15
Sensibilitate la recepție	802.11a: -72 dBm (tipic) la 54 Mb/s 802.11b: -85 dBm (tipic) la 11 Mb/s 802.11g: -73 dBm (tipic) la 54 Mb/s 802.11n (20 MHz): -75 dBm (tipic) la MCS15 802.11n (40 MHz): -69 dBm (tipic) la MCS15
Amplificare antenă în dBi	1
Securitate fără fir	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Biți cheie de securitate	Criptare până la 128 de biți

Cerințe de mediu

Dimensiuni	6,97" x 5,04" x 2,68" (177 x 128 x 68 mm)
Greutate	0,65 lb (295 g)
Certificare	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentare	12 V, 1 A
Temperatură de funcționare	32 - 104 ºF (0 - 40 ºC)
Temperatură de depozitare	-4 - 140 ºF (-20 - 60 ºC)
Umiditate de funcționare	Între 10 și 85% fără condens
Umiditate de depozitare	Între 5 și 90% fără condens

Specificațiile pot fi modificate fără preaviz.

WET610N

Model	WET610N
Standarde	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED-uri	Alimentare, Ethernet, Wi-Fi Protected Setup™, Fără fir
Porturi	Ethernet, Alimentare
Butoane	Resetare, Wi-Fi Protected Setup
Tip de cablaj	CAT5e
Antene	3 (interne)
Tip de conector la antenă	N/A
Detașabil (Da/Nu)	Nu
Modulații	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Putere RF (EIRP) în dBm	802.11a: 15 dBm (tipic) la 54 Mb/s 802.11b: 18 dBm (tipic) la 11 Mb/s 802.11g: 16 dBm (tipic) la 54 Mb/s 802.11n: 12 dBm (tipic) la 130 Mbps (HT20), 270 Mb/s (HT40)
Sensibilitate la recepție	802.11a: -72 dBm (tipic) la 54 Mb/s 802.11b: -85 dBm (tipic) la 11 Mb/s 802.11g: -73 dBm (tipic) la 54 Mb/s 802.11n: -70 dBm (tipic) la MCS15/2,4 GHz, -69 dBm (tipic) la MCS15/5,0 GHz
Amplificare antenă în dBi	1
Securitate fără fir	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Biți cheie de securitate	Criptare până la 128 de biți

Cerințe de mediu

Dimensiuni	5,71" x 4,17" x 2,05" (145 x 106 x 52 mm)
Greutate	5,61 oz (159 g)
Certificare	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Alimentare	12 V, 1 A
Temperatură de funcționare	32 - 104 ºF (0 - 40 ºC)
Temperatură de depozitare	-4 - 140 ºF (-20 - 60 ºC)
Umiditate de funcționare	Între 10 și 85% fără condens
Umiditate de depozitare	Între 5 și 90% fără condens

Specificațiile pot fi modificate fără notificare.

Linksys.com/support

Cisco, sigla Cisco și Linksys sunt mărci comerciale sau mărci comerciale înregistrate ale Cisco și/sau ale filialelor acesteia în Statele Unite ale Americii și în alte țări.
O listă a mărcilor comerciale Cisco poate fi găsită la adresa www.cisco.com/go/trademarks. Toate celelalte mărci comerciale menționate în acest document aparțin proprietarilor respectivi.

© 2011 Cisco și/sau afiliații săi. Toate drepturile sunt rezervate.

3425-01249



Руководство пользователя

Linksys WET610N/WES610N | Двухдиапазонный мост N Entertainment

Содержание

Обзор продукта

Панель индикаторов 2
Задняя панель 3

Меры по защите беспроводных сетей

Изменение имени беспроводной сети/идентификатора SSID по умолчанию 4
Изменение пароля по умолчанию 4
Включение фильтрации MAC-адресов 4
Включение шифрования 4

Общие указания по защите беспроводных сетей. 4
Дополнительные советы по защите сетей 5

Расширенная конфигурация

Доступ к веб-утилите моста 6
Setup (Настройка) > Basic Setup (Основные настройки) 7
Language (Язык) 7
Настройка сети 7

Wireless (Беспроводная сеть) > Basic Wireless Settings (Основные настройки беспроводной сети). 7
сновные настройки беспроводной сети 8
Безопасность беспроводной сети 8
Режим обеспечения безопасности 8
i-Fi Protected Setup 9

Wireless (Беспроводная сеть) > Wireless Network Site Survey (Беспроводная сеть – обследование объекта). . . . 10
Беспроводная сеть – обследование объекта 10

Wireless (Беспроводная сеть) > WMM® 11
WMM 12

Wireless (Беспроводная сеть) > Advanced Wireless Settings (Дополнительные настройки беспроводной сети) 13
Дополнительные функции беспроводной сети 14

Administration (Администрирование) > Management (Управление) 14
Управление 14

Administration (Администрирование) > Factory Defaults (Заводские настройки) 15
Заводские настройки 15

Administration (Администрирование) > Upgrade Firmware (Обновить прошивку) 15
Upgrade Firmware (Обновить прошивку) 15

Status (Состояние) > Bridge (Мост). 15
Bridge Information (Сведения о мосте) 16
Локальная сеть 16

Status (Состояние) > Wireless (Беспроводная сеть) 16
Беспроводная сеть 16

Поиск и устранение неполадок

WES610N/WET610N 17

Технические характеристики

WES610N 18
WET610N 19

Обзор продукта

Благодарим вас за выбор двухдиапазонного моста Linksys N Entertainment. Мост позволяет подключать любые проводные Ethernet-устройства к беспроводной сети. Мост использует двухдиапазонный режим Wireless-N, поэтому он совместим с любыми маршрутизаторами и точками доступа Wireless-N, -G, -A или -B. Для первоначальной установки следуйте инструкциям на компакт-диске. Для настройки дополнительных параметров используйте удобную веб-утилиту.

Панель индикаторов



WES610N WET610N

Беспроводная связь (синий) Индикатор беспроводной связи загорается при установлении беспроводного соединения. Этот индикатор мигает, когда мост активно передает или принимает данные по беспроводной сети.

Кнопка Wi-Fi Protected Setup Если маршрутизатор поддерживает функцию Wi-Fi Protected Setup и использует режим безопасности WPA или WPA2, то можно использовать функцию WiFi Protected Setup для подключения к мосту в автоматическом режиме. Для использования функции Wi-Fi Protected Setup ознакомьтесь с разделом "Wireless (Беспроводная сеть) > Basic Wireless Settings (Основные настройки беспроводной сети)" на стр. 7.

Индикатор Wi-Fi Protected Setup (синий/желтый) Этот индикатор мигает синим цветом в течение двух минут во время активации функции Wi-Fi Protected Setup. Когда защита беспроводной сети активирована, индикатор загорается синим цветом. Если в процессе активации функции Wi-Fi Protected Setup возникает ошибка, то этот индикатор загорается желтым цветом. Убедитесь, что сетевой маршрутизатор поддерживает функцию Wi-Fi Protected Setup. Подождите, пока индикатор погаснет, а затем попробуйте активировать эту функцию еще раз.

Ethernet (синий) Индикатор Ethernet загорается при установлении проводного соединения. Этот индикатор мигает, когда мост активно передает или принимает данные через порт(ы) Ethernet.

Power (Питание) (синий) Индикатор питания загорается при включении питания моста.

Задняя панель



WES610N WET610N

Ethernet Порты Ethernet используются для подключения моста к компьютеру или другому сетевому Ethernet-устройству. WES610N имеет четыре порта, а WET610N имеет один порт.

Reset (Сброс) Существует два способа восстановления заводских настроек моста. Нажмите и удерживайте кнопку Reset (Сброс) в течение примерно 5 секунд либо восстановите значения по умолчанию с помощью пункта меню Administration (Администрирование) > Factory Defaults (Заводские настройки) веб-утилиты моста. Кнопка Reset (Сброс) расположена на нижней панели WES610N и на задней панели WET610N.

Power (Питание) Гнездо питания служит для подключения входящего в комплект поставки сетевого адаптера.

Меры по защите беспроводных сетей

Беспроводные сети удобны и просты в установке. Сегодня в связи с широким распространением технологий высокоскоростного доступа в Интернет такие сети развиваются стремительными темпами. Поскольку в беспроводных сетях передача информации осуществляется с использованием радиоволн, они гораздо уязвимее для попыток несанкционированного доступа, чем традиционные проводные сети. Как и сигналы мобильных и радиотелефонов, сигналы беспроводных сетевых устройств могут быть перехвачены. Так как предотвратить нежелательное подключение к беспроводной сети физически невозможно, для обеспечения безопасности необходимо предпринять дополнительные меры.

Изменение имени беспроводной сети/ идентификатора SSID по умолчанию

При изготовлении каждому беспроводному устройству присваивается имя (идентификатор SSID) по умолчанию. Это имя вашей беспроводной сети. Оно может содержать до 32 символов. В беспроводных устройствах Linksys в качестве имени беспроводной сети по умолчанию используется слово **linksys**. Для того чтобы вашу беспроводную сеть можно было отличить от других беспроводных сетей, находящихся поблизости, следует изменить имя по умолчанию на какое-либо другое уникальное имя. Однако при составлении имени не следует использовать свои персональные данные (например, номер паспорта), так как эта информация может стать известна другим людям, осуществляющим поиск доступных беспроводных сетей.

Изменение пароля по умолчанию

При попытке изменить настройки беспроводных устройств (точек доступа и маршрутизаторов) запрашивается пароль. При изготовлении на таких устройствах устанавливается пароль по умолчанию. Стандартным паролем устройств Linksys является **admin**. Хакерам известны эти установки по умолчанию, и с их помощью они могут попытаться получить доступ к вашему беспроводному устройству и изменить ваши сетевые настройки. Чтобы воспрепятствовать любым несанкционированным изменениям, используйте такой пароль, который будет трудно подобрать.

Включение фильтрации MAC-адресов

Маршрутизаторы Linksys позволяют активировать фильтрацию MAC-адресов. MAC-адрес представляет собой уникальную последовательность букв и цифр, назначаемую каждому сетевому устройству. При включенной фильтрации MAC-адресов доступ к беспроводной сети предоставляется только беспроводным устройствам с заданными MAC-адресами. Например, можно задать MAC-адреса всех домашних компьютеров, чтобы доступ к вашей беспроводной сети предоставлялся только этим компьютерам.

Включение шифрования

Шифрование позволяет защитить данные, передаваемые по беспроводной сети. Защищенный WiFi-доступ (по протоколу WPA/WPA2) и шифрование с помощью WEP-ключей обеспечивают разные уровни защиты беспроводного трафика.

Шифрование по протоколу WPA/WPA2 обеспечивает большую безопасность по сравнению с шифрованием на базе WEP-ключей, поскольку протокол WPA/WPA2 подразумевает использование динамических ключей. Для защиты информации, передаваемой в радиочастотном диапазоне, следует установить самый высокий уровень шифрования, поддерживаемый вашим сетевым оборудованием.

WEP – это более старый стандарт шифрования, и для некоторых не очень современных устройств, не поддерживающих протокол WPA, этот вариант может оказаться единственно возможным.

Общие указания по защите беспроводных сетей

Обеспечение безопасности беспроводного трафика не имеет смысла, если не защищена базовая сеть.

- Защитите паролем все компьютеры в сети; отдельным паролем защитите файлы, содержащие конфиденциальную информацию.
- Регулярно меняйте пароли.
- Установите антивирусное ПО и персональный межсетевой экран.
- Обязательно отключите возможность совместного использования файлов (в одноранговой сети). Помните, что некоторые приложения могут активировать совместный доступ к файлам без вашего разрешения и/или ведома.

Дополнительные советы по защите сетей

- Такое оборудование, как беспроводные маршрутизаторы, точки доступа и шлюзы, должно находиться вдали от внешних стен и окон.
- Выключайте беспроводные маршрутизаторы, точки доступа и шлюзы, когда они не используются (например, на ночь или на время вашего отпуска).
- Используйте парольные фразы, состоящие не менее чем из восьми символов. Комбинируйте буквы и цифры; старайтесь не пользоваться стандартными словами, которые можно найти в словаре.

Расширенная конфигурация

После настройки с помощью инструкций на компакт-диске мост готов к работе. Однако при необходимости изменить дополнительные параметры следует воспользоваться веб-утилитой настройки моста. В данной главе описываются все веб-страницы данной утилиты и ключевые функции, доступные на каждой странице. Доступ к данной утилите можно осуществить с помощью веб-браузера с компьютера, объединенного с мостом в одну локальную сеть.

Эта утилита содержит следующие основные вкладки: Setup (Настройка), Wireless (Беспроводная сеть), Administration (Администрирование) и Status (Состояние). После перехода на одну из основных вкладок открываются дополнительные вкладки.

Доступ к веб-утилите моста

Используйте веб-браузер для доступа к веб-утилите.

Если мост подключен к сети с DHCP-сервером (его роль, как правило, выполняет сетевой маршрутизатор), то свой IP-адрес он получит от DHCP-сервера. Если в сети нет DHCP-сервера, то мост использует статический IP-адрес по умолчанию: **169.254.1.250**. (Если при помощи веб-утилиты для моста установлен постоянный статический IP-адрес, то введите этот статический IP-адрес.)

ПРИМЕЧАНИЕ
Если вы не знаете IP-адрес моста, вы можете найти его в таблице DHCP-клиентов маршрутизатора. (См. документацию к маршрутизатору.)

Если вы не можете найти IP-адрес моста, вы можете сбросить настройки моста; при помощи выпрямленной канцелярской скрепки нажмите кнопку **Reset** (Сброс) на мосте и удерживайте ее приблизительно пять секунд. Настройки моста будут сброшены до заводских значений, используемых по умолчанию. Мост запросит IP-адрес у DHCP-сервера (его роль, как правило, выполняет сетевой маршрутизатор). Если DHCP-сервер не найден, то мост будет использовать статический IP-адрес по умолчанию (**169.254.1.250**), пока DHCP-сервер не будет обнаружен и динамический IP-адрес не будет назначен.

Если мост не связан с маршрутизатором и использует заводские настройки, подключите компьютер непосредственно к мосту при помощи соединения Ethernet, затем откройте веб-утилиту. Для этого потребуется настроить соединение Ethernet компьютера для использования статического IP-адреса и маски подсети.

Для Ethernet-адаптера необходимо установить определенный IP-адрес.

1. В поле *IP address* (IP-адрес) введите **169.254.x.y** (x следует заменить числом от 1 до 254, а y следует заменить числом от 0 до 255).
2. В поле *Subnet mask* (Маска подсети) введите **255.255.0.0**.

ПРИМЕЧАНИЕ
Действия, которые необходимо выполнить для назначения IP-адреса Ethernet-адаптеру компьютера, зависят от операционной системы. Для получения инструкций см. справочную документацию для вашей операционной системы.

После того, как Ethernet-адаптеру назначен статический IP-адрес, запустите веб-браузер, затем введите IP-адрес адаптера (значение по умолчанию: **169.254.1.250**) в поле *Address* (Адрес). Нажмите клавишу **Enter**.

Появляется экран запроса пароля. (Подобный экран появляется и в среде систем, отличных от Windows XP.) Не заполняйте поле *Имя пользователя*. Введите пароль, созданный в процессе работы мастера установки. Если вы не создавали нового пароля, используйте пароль по умолчанию – **admin**. (Новый пароль можно установить на экране *Administration (Администрирование)* > *Management (Управление).*) Для продолжения нажмите кнопку **OK**.



ПРИМЕЧАНИЕ
Если экран ввода пароля не отображается, подождите две минуты и повторите попытку.

Setup (Настройка) > Basic Setup (Основные настройки)

Сначала появляется экран *Basic Setup* (Основные настройки). На этом экране можно изменить язык интерфейса веб-утилиты или настроить параметры моста для проводной сети Ethernet.





Language (Язык)

Language (Язык) Это поле используется для установки языка отображаемого на экране интерфейса веб-утилиты. Выберите требуемый язык в выпадающем меню.

Настройка сети

Этот раздел определяет, выдается ли IP-адрес моста DHCP-сервером (например, сетевым маршрутизатором) в автоматическом режиме (Автоматическая конфигурация – DHCP) или же адрес задается вручную (Статический IP-адрес).

Bridge IP (IP-адрес моста) Если в вашей сети имеется DHCP-сервер, такой, например, как сетевой маршрутизатор, выдающий IP-адреса всем сетевым устройствам, то для этого параметра оставьте значение по умолчанию – **Automatic Configuration – DHCP** (Автоматическая конфигурация – DHCP). Мост запросит IP-адрес у DHCP-сервера (его роль, как правило, выполняет сетевой маршрутизатор). Если DHCP-сервер не найден, то мост будет использовать статический IP-адрес по умолчанию (**169.254.1.250**), пока DHCP-сервер не будет обнаружен и динамический IP-адрес не будет назначен.

Если же вы хотите установить для моста постоянный статический IP-адрес, выберите для этого параметра значение **Static IP** (Статический IP-адрес).

В случае выбора варианта Static IP (Статический IP-адрес) заполните следующие поля.

- **Static IP Address (Статический IP-адрес)** Введите уникальный IP-адрес, который будет использоваться для доступа к веб-утилите.
- **Subnet Mask (Маска подсети)** Введите маску подсети вашей проводной сети.
- **Default Gateway (Основной шлюз)** Введите IP-адрес основного шлюза вашей сети (в большинстве случае им является маршрутизатор).

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

Wireless (Беспроводная сеть) > Basic Wireless Settings (Основные настройки беспроводной сети)

Экран *Basic Wireless Settings* (Основные настройки беспроводной сети) используется для настройки основных параметров беспроводной сети и обеспечения ее безопасности.

Существует два способа настройки параметров моста: вручную или с помощью функции Wi-Fi Protected Setup (Защищенная настройка Wi-Fi). Функция Wi-Fi Protected Setup позволяет достаточно легко настроить беспроводную сеть. Если сетевой маршрутизатор поддерживает функцию Wi-Fi Protected Setup и использует режим безопасности WPA или WPA2, то можно использовать функцию Wi-Fi Protected Setup для подключения к мосту в автоматическом режиме.

Configuration View (Просмотр конфигурации) Для ручной настройки беспроводной сети выберите **Manual** (Вручную). Перейдите к разделу **Basic Wireless Settings** (Основные настройки беспроводной сети) **на стр. 8**. Для использования функции Wi-Fi Protected Setup выберите **Wi-Fi Protected Setup**. Перейдите к разделу **Wi-Fi Protected Setup** **на стр. 9**.

сновные настройки беспроводной сети



Network Name (SSID) (Сетевое имя (SSID)) SSID это имя сети, используемое всеми точками доступа беспроводной сети. Имя сети должно быть одинаковым для всех устройств в беспроводной сети. Сетевое имя должно вводиться с учетом регистра, количество символов не должно превышать 32 (любые символы, доступные на клавиатуре). Убедитесь, что эта настройка совпадает с настройкой беспроводной маршрутизатора или точки доступа. В целях повышения безопасности рекомендуется SSID по умолчанию (**linksys**) заменить уникальным именем.

Безопасность беспроводной сети

Данная модель моста поддерживает следующие режимы обеспечения безопасности беспроводной сети: WPA Personal, WPA2 Personal и WEP. WPA (Wi-Fi Protected Access) (Защищенный доступ к Wi Fi) и WPA2 являются более стойкими алгоритмами защиты, чем WEP (Wired Equivalent Privacy). Более подробная информация о безопасности беспроводной сети представлена в разделе "Контрольный перечень мер по обеспечению безопасности беспроводных сетей" на стр. 4.

Режим обеспечения безопасности

Выберите метод обеспечения безопасности в беспроводной сети. Если нет необходимости использовать средства обеспечения безопасности беспроводной сети, сохраните значение по умолчанию – **Disabled** (Отключено).

ПРИМЕЧАНИЕ
Обратите внимание на то, что все устройства, подключенные к беспроводной сети, ДОЛЖНЫ использовать один и тот же режим обеспечения безопасности и парольную фразу (или ключ), иначе беспроводные устройства не смогут взаимодействовать друг с другом.

WPA Personal

WPA – стандарт безопасности, обеспечивающий более высокий уровень защиты по сравнению с протоколом шифрования WEP.



Encryption (Шифрование) Протокол WPA поддерживает метод шифрования TKIP с динамическими ключами шифрования.

Passphrase (Парольная фраза) Введите ключ, используемый мостом и беспроводным маршрутизатором (точкой доступа). Он должен содержать 8–63 символа.

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

WPA2 Personal

WPA2 является дальнейшим развитием алгоритма защиты WPA.



Encryption (Шифрование) Протокол WPA2 поддерживает два метода шифрования, TKIP и AES, с динамическими ключами шифрования. Выберите метод шифрования, **AES** или **TKIP or AES** (TKIP или AES). По умолчанию установлено значение **AES** (TKIP или AES).

Passphrase (Парольная фраза) Введите ключ, используемый мостом и беспроводным маршрутизатором (точкой доступа). Он должен содержать 8–63 символа.

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

WEP

WEP является основным методом шифрования, который не столь надежен, как WPA или WPA2.



Encryption (Шифрование) Выберите уровень шифрования WEP, **40/64 -битное (10 шестнадцатеричных цифр)** или **104/128-битное (26 шестнадцатеричных цифр)**. По умолчанию устанавливается режим **40/64 bits (10 hex digits) (40/64-битное, 10 шестнадцатеричных цифр)**.

Key 1 (Ключ 1) Введите WEP-ключ для своей сети.

Tx Key (Ключ передачи) **Key 1 (Ключ 1)** является передающим ключом, используемым мостом.

Authentication Type (Тип аутентификации) По умолчанию установлен режим **Auto** (Авто), который разрешает только аутентификацию в режиме Open System (Открытая система) или Shared Key (Общий ключ). Выберите **Open** (Открытая) для использования аутентификации "открытая система"; отправитель и получатель не используют WEP-ключ для аутентификации. Выберите **Shared** (Общий) для использования аутентификации "общий ключ"; отправитель и получатель используют WEP-ключ для аутентификации.

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

i-Fi Protected Setup

Существует два способа настройки этой функции. Используйте тот способ, который подходит для используемого маршрутизатора.





Способ 1

Используйте этот способ, если маршрутизатор оснащен кнопкой Wi-Fi Protected Setup.

1. Нажмите кнопку **Wi-Fi Protected Setup** на маршрутизаторе.
2. В течение двух минут после этого нажмите кнопку **Wi-Fi Protected Setup** на экране *Wi-Fi Protected Setup* (Защищенная настройка Wi-Fi) веб-утилиты моста.
3. После настройки моста нажмите кнопку **Close** (Закрыть).

На экране *Wi-Fi Protected Setup* (Защищенная настройка Wi-Fi) отображается состояние канала, сетевое имя (SSID) и метод обеспечения безопасности.

Способ 2

Используйте этот способ, если маршрутизатор требует ввода PIN-кода моста.

1. На экране **маршрутизатора** *Wi-Fi Protected Setup* (Защищенная настройка Wi-Fi) введите PIN-код, указанный на экране **Wi-Fi Protected Setup** (Защищенная настройка Wi-Fi) *веб-утилиты моста*. Затем нажмите кнопку **Register** (Зарегистрировать) или другую соответствующую кнопку. (Он также указан на этикетке, прикрепленной в нижней части моста.)
2. На **экране** *Wi-Fi Protected Setup* (Защищенная настройка Wi-Fi) нажмите **OK**.
3. После настройки моста нажмите кнопку **Close** (Закрыть).

На экране *Wi-Fi Protected Setup* (Защищенная настройка Wi-Fi) отображается состояние канала, сетевое имя (SSID) и метод обеспечения безопасности.

Wireless (Беспроводная сеть) > Wireless Network Site Survey (Беспроводная сеть – обследование объекта)

Перейдите на вкладку **Wireless Network Site Survey** (Беспроводная сеть – обследование объекта), чтобы начать обследование объекта. Экран *Wireless Network Site Survey* (Беспроводная сеть – обследование объекта) содержит перечень беспроводных сетей, обнаруженных мостом.



Беспроводная сеть – обследование объекта

Number of Wireless Networks (Число беспроводных сетей) Отображается число беспроводных сетей, обнаруженных мостом.

Select (Выбрать) Чтобы подключиться к беспроводной сети, нажмите **Select** (Выбрать). Затем нажмите кнопку **Connect** (Подключиться).

Wireless Network Name (Имя беспроводной сети) Отображается сетевое имя (SSID) беспроводной сети.

GHz (ГГц) Отображается радиодиапазон беспроводной сети.

Signal (Сигнал) Отображается уровень сигнала в процентном соотношении. Значение 100 % указывает на самый высокий уровень сигнала; 0 % указывает на самый низкий уровень сигнала.

Security (Безопасность) Если сеть поддерживает функцию Wi-Fi Protected Setup, то отображается значок Wi-Fi Protected Setup (Защищенная настройка Wi-Fi) . Отображается используемый метод обеспечения безопасности беспроводной сети.

Для обновления информации, отображаемой на экране, нажмите кнопку **Refresh** (Обновить).

После того, как сеть выбрана, нажмите **Connect** (Подключиться). Откроется новый экран. Следуйте инструкциям для режима безопасности, используемого в сети.

WPA



Network Name (SSID) Сетевое имя (SSID) Автоматически отображается имя выбранной сети.

Security Mode (Режим безопасности) Автоматически отображается WPA Personal.

Encryption (Шифрование) Протокол WPA поддерживает метод шифрования TKIP с динамическими ключами шифрования.

Passphrase (Парольная фраза) Введите ключ, используемый мостом и беспроводным маршрутизатором (точкой доступа). Он должен содержать 8–63 символа.

Для обновления информации, отображаемой на экране, нажмите кнопку **Refresh** (Обновить).

После ввода настроек безопасности нажмите **Connect** (Подключиться).

WPA2



Network Name (SSID) Сетевое имя (SSID) Автоматически отображается имя выбранной сети.

Security Mode (Режим безопасности) Автоматически отображается WPA2 Personal.

Encryption (Шифрование) Протокол WPA2 поддерживает два метода шифрования, TKIP и AES, с динамическими ключами шифрования. Выберите метод шифрования, AES **или TKIP or** AES **(TKIP или AES).**

Passphrase (Парольная фраза) Введите ключ, используемый мостом и беспроводным маршрутизатором (точкой доступа). Он должен содержать 8–63 символа.

Для обновления информации, отображаемой на экране, нажмите кнопку **Refresh** (Обновить).

После ввода настроек безопасности нажмите **Connect** (Подключиться).

WEP



Network Name (SSID) Сетевое имя (SSID) Автоматически отображается имя выбранной сети.

Security Mode (Режим безопасности) Автоматически отображается WEP.

Encryption(Шифрование) Выберите уровень шифрования WEP: **40/64 bits (10 hex digits)** (40/64 бита (10 шестнадцатеричных цифр)) или **104/128 bits (26 hex digits)** (104/128 битов (26 шестнадцатеричных цифр)).

Key 1 (Ключ 1) Введите WEP-ключ для своей сети.

Tx Key (Ключ передачи) **Key 1 (Ключ 1)** является передающим ключом, используемым мостом.

Authentication Type (Тип аутентификации) По умолчанию установлен режим **Auto** (Авто), который разрешает только аутентификацию в режиме Open System (Открытая система) или Shared Key (Общий ключ). Выберите **Open** (Открытая) для использования аутентификации "открытая система"; отправитель и получатель не используют WEP-ключ для аутентификации. Выберите **Shared** (Общий) для использования аутентификации "общий ключ"; отправитель и получатель используют WEP-ключ для аутентификации.

Для обновления информации, отображаемой на экране, нажмите кнопку **Refresh** (Обновить).

После ввода настроек безопасности нажмите **Connect** (Подключиться).

Wireless (Беспроводная сеть) > WMM®

Настройте параметры Wireless MultiMedia (WMM) (Поддержка протокола WWM). Протокол WMM определяет приоритетность пакетов в зависимости от соответствующих им режимов доступа (типов трафика): Background (Фоновый), Best Effort (Максимальный), Video (Видео) или Voice (Голосовой). Настройка этих параметров должна выполняться только опытным администратором, поскольку их неправильный выбор может заметно ухудшить производительность беспроводной сети.



ПРИМЕЧАНИЕ
Настройки на экране *WMM* предназначены только для опытных пользователей.

WMM

Access Mode (Режим доступа)

Параметры для каждого из четырех существующих режимов доступа можно настраивать отдельно. Выберите режим, который требуется настроить: **Background** (Фоновый), **Best Effort** (Максимальный), **Video** (Видео) или **Voice** (Голосовой). Следуйте инструкциям для выбранного режима.

Background (Фоновый)

Use Aggregation (Использование агрегации) Этот параметр определяет, будет ли на уровне управления доступом к среде передаче (MAC; Media Access Control) устанавливаться сеанс подтверждения приема блока кадров (ADDBA; Add Block Acknowledgement). По умолчанию установлено значение **No** (Нет). Чтобы активировать эту функцию, установите значение **Yes** (Да).

Accept Aggregation (Принимать агрегации) Этот параметр определяет, будут ли на MAC-уровне приниматься запросы ADDBA. По умолчанию установлено значение **Yes** (Да). Чтобы выключить эту функцию, установите значение **No** (Нет).

Max. Number of Packets in Aggregation (Макс. количество пакетов в агрегации) Этот параметр определяет максимальное количество пакетов (суб-кадров) в одной агрегации. Диапазон действительных значений: от **0** до **7**. По умолчанию установлено значение **7**.

Max. Aggregation Size (Макс. размер агрегации) Этот параметр определяет максимальный размер агрегации (в байтах). Диапазон действительных значений: от **0** до **16000**. По умолчанию установлено значение **12000**.

Timeout Interval (Продолжительность времени ожидания) Этот параметр определяет длительность периода времени, по истечении которого агрегация должна быть закрыта по "условию закрытия", прежде чем она будет аннулирована таймером. Диапазон действительных значений: от **0** до **100** мс. По умолчанию установлено значение **3**.

Min. Size of Packet in Aggregation (Мин. размер пакета в агрегации) Этот параметр определяет минимальный размер пакетов (в байтах), которые могут быть аккумулированы в агрегации. Диапазон действительных значений: от **0** до **1500**. По умолчанию установлено значение **10**.

ADDBA Timeout (Время ожидания ADDBA) Этот параметр определяет длительность периода времени, по истечении которого установление ADDBA прекращается, если за указанное время ни разу не был осуществлен обмен кадрами с использованием протокола подтверждения приема блока кадров (Block ACK). Диапазон действительных значений: от **0** до **65535** мс. По умолчанию установлено значение **0**, то есть время ожидания не ограничено.

Aggregation Window Size (Размер окна агрегации) Этот параметр определяет максимальное количество пакетов, передаваемых без получения подтверждений (ACK). Диапазон действительных значений: от **0** до **64**. По умолчанию установлено значение **64**.

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

Best Effort (Максимальный)

Use Aggregation (Использование агрегации) Этот параметр определяет, будет ли на уровне управления доступом к среде передаче (MAC; Media Access Control) устанавливаться сеанс подтверждения приема блока кадров (ADDBA; Add Block Acknowledgement). По умолчанию установлено значение **Yes** (Да). Чтобы выключить эту функцию, установите значение **No** (Нет).

Accept Aggregation (Принимать агрегации) Этот параметр определяет, будут ли на MAC-уровне приниматься запросы ADDBA. По умолчанию установлено значение **Yes** (Да). Чтобы выключить эту функцию, установите значение **No** (Нет).

Max. Number of Packets in Aggregation (Макс. количество пакетов в агрегации) Этот параметр определяет максимальное количество пакетов (суб-кадров) в одной агрегации. Диапазон действительных значений: от **0** до **10**. По умолчанию установлено значение **10**.

Max. Aggregation Size (Макс. размер агрегации) Этот параметр определяет максимальный размер агрегации (в байтах). Диапазон действительных значений: от **0** до **20000**. По умолчанию установлено значение **16000**.

Timeout Interval (Продолжительность времени ожидания) Этот параметр определяет длительность периода времени, по истечении которого агрегация должна быть закрыта по "условию закрытия", прежде чем она будет аннулирована таймером. Диапазон действительных значений: от **0** до **100** мс. По умолчанию установлено значение **3**.

Min. Size of Packet in Aggregation (Мин. размер пакета в агрегации) Этот параметр определяет минимальный размер пакетов (в байтах), которые могут быть аккумулированы в агрегации. Диапазон действительных значений: от **0** до **1500**. По умолчанию установлено значение **10**.

ADDBA Timeout (Время ожидания ADDBA) Этот параметр определяет длительность периода времени, по истечении которого установление ADDBA прекращается, если за указанное время ни разу не был осуществлен обмен кадрами с использованием протокола подтверждения приема блока кадров (Block ACK). Диапазон действительных значений: от **0** до **65535** мс. По умолчанию установлено значение **0**, то есть время ожидания не ограничено.

Aggregation Window Size (Размер окна агрегации) Этот параметр определяет максимальное количество пакетов, передаваемых без получения подтверждений (ACK). Диапазон действительных значений: от **0** до **64**. По умолчанию установлено значение **64**.

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

Video (Видео)

Use Aggregation (Использование агрегации) Этот параметр определяет, будет ли на уровне управления доступом к среде передаче (MAC; Media Access Control) устанавливаться сеанс подтверждения приема блока кадров (ADDBA; Add Block Acknowledgement). По умолчанию установлено значение **Yes** (Да). Чтобы выключить эту функцию, установите значение **No** (Нет).

Accept Aggregation (Принимать агрегации) Этот параметр определяет, будут ли на MAC-уровне приниматься запросы ADDBA. По умолчанию установлено значение **Yes** (Да). Чтобы выключить эту функцию, установите значение **No** (Нет).

Max. Number of Packets in Aggregation (Макс. количество пакетов в агрегации) Этот параметр определяет максимальное количество пакетов (суб-кадров) в одной агрегации. Диапазон действительных значений: от **0** до **7**. По умолчанию установлено значение **7**.

Max. Aggregation Size (Макс. размер агрегации) Этот параметр определяет максимальный размер агрегации (в байтах). Диапазон действительных значений: от **0** до **16000**. По умолчанию установлено значение **12000**.

Timeout Interval (Продолжительность времени ожидания) Этот параметр определяет длительность периода времени, по истечении которого агрегация должна быть закрыта по "условию закрытия", прежде чем она будет аннулирована таймером. Диапазон действительных значений: от **0** до **100** мс. По умолчанию установлено значение **3**.

Min. Size of Packet in Aggregation (Мин. размер пакета в агрегации) Этот параметр определяет минимальный размер пакетов (в байтах), которые могут быть аккумулированы в агрегации. Диапазон действительных значений: от **0** до **1500**. По умолчанию установлено значение **10**.

ADDBA Timeout (Время ожидания ADDBA) Этот параметр определяет длительность периода времени, по истечении которого установление ADDBA прекращается, если за указанное время ни разу не был осуществлен обмен кадрами с использованием протокола подтверждения приема блока кадров (Block ACK). Диапазон действительных значений: от **0** до **65535** мс. По умолчанию установлено значение **0**, то есть время ожидания не ограничено.

Aggregation Window Size (Размер окна агрегации) Этот параметр определяет максимальное количество пакетов, передаваемых без получения подтверждений (ACK). Диапазон действительных значений: от **0** до **64**. По умолчанию установлено значение **64**.

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

Voice (Голосовой)

Use Aggregation (Использование агрегации) Этот параметр определяет, будет ли на уровне управления доступом к среде передаче (MAC; Media Access Control) устанавливаться сеанс подтверждения приема блока кадров (ADDBA; Add Block Acknowledgement). По умолчанию установлено значение **Yes** (Да). Чтобы выключить эту функцию, установите значение **No** (Нет).

Accept Aggregation (Принимать агрегации) Этот параметр определяет, будут ли на MAC-уровне приниматься запросы ADDBA. По умолчанию установлено значение **Yes** (Да). Чтобы выключить эту функцию, установите значение **No** (Нет).

Max. Number of Packets in Aggregation (Макс. количество пакетов в агрегации) Этот параметр определяет максимальное количество пакетов (суб-кадров) в одной агрегации. Диапазон действительных значений: от **0** до **2**. По умолчанию установлено значение **2**.

Max. Aggregation Size (Макс. размер агрегации) Этот параметр определяет максимальный размер агрегации (в байтах). Диапазон действительных значений: от **0** до **16000**. По умолчанию установлено значение **10000**.

Timeout Interval (Продолжительность времени ожидания) Этот параметр определяет длительность периода времени, по истечении которого агрегация должна быть закрыта по "условию закрытия", прежде чем она будет аннулирована таймером. Диапазон действительных значений: от **0** до **100** мс. По умолчанию установлено значение **10**.

Min. Size of Packet in Aggregation (Мин. размер пакета в агрегации) Этот параметр определяет минимальный размер пакетов (в байтах), которые могут быть аккумулированы в агрегации. Диапазон действительных значений: от **0** до **1500**. По умолчанию установлено значение **10**.

ADDBA Timeout (Время ожидания ADDBA) Этот параметр определяет длительность периода времени, по истечении которого установление ADDBA прекращается, если за указанное время ни разу не был осуществлен обмен кадрами с использованием протокола подтверждения приема блока кадров (Block ACK). Диапазон действительных значений: от **0** до **65535** мс. По умолчанию установлено значение **0**, то есть время ожидания не ограничено.

Aggregation Window Size (Размер окна агрегации) Этот параметр определяет максимальное количество пакетов, передаваемых без получения подтверждений (ACK). Диапазон действительных значений: от **0** до **64**. По умолчанию установлено значение **64**.

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

Wireless (Беспроводная сеть) > Advanced Wireless Settings (Дополнительные настройки беспроводной сети)

Настройте дополнительные функции беспроводной сети моста. Настройка этих параметров должна выполняться только опытным администратором, поскольку их неправильный выбор может заметно ухудшить производительность беспроводной сети.



ПРИМЕЧАНИЕ

Настройки на экране *Advanced Wireless Settings* (Дополнительные настройки беспроводной сети) предназначены только для опытных пользователей.

Дополнительные функции беспроводной сети

Use LDPC (Использовать LDPC) Код LDPC (код низкой плотности с контролем на четность) позволяет включить или отключить функцию исправления ошибок для снижения риска потери данных в каналах с высоким уровнем помех. Алгоритм адаптации скорости передачи данных автоматически отключает код LDPC при высоких физических скоростях (выше 162). Чтобы использовать расширенную схему исправления ошибок LDCP, оставьте значение по умолчанию: **Yes**. В противном случае выберите **Нет**.

ERP Protection Type (Тип защиты ERP) Этот параметр позволяет настроить защиту пакетов OFDM независимо от наличия станций 802.11b в беспроводной сети. Отправляя пакеты RTS/CTS или CTS2Self на скорости 802.11b, мост сообщает беспроводной сети, что пакеты OFDM будут переданы, и защищает эти пакеты в беспроводной сети. Пакеты RTS/CTS и CTS2Self создают непроизводительные потери, которые могут снизить пропускную способность сети.

Параметр RTS/CTS обеспечивает улучшенное покрытие, но снижает пропускную способность сети по сравнению с параметром CTS2Self, поскольку параметр RTS/CTS требует подтверждения от принимающего устройства. Чтобы использовать функцию RTS/CTS, оставьте значение по умолчанию, **RTS/CTS**. Параметр None (Нет) может вызвать конфликты между пакетами OFDM и CCK. Чтобы использовать этот параметр, выберите **None** (Нет). Чтобы использовать параметр CTS2Self, выберите **CTS2Self**.

11n Protection Type (Тип защиты 11n) Этот параметр настраивает защиту от устройств с низкой пропускной способностью в беспроводной сети. Если беспроводной маршрутизатор (или точка доступа) обнаруживает подключение устройства с низкой пропускной способностью предыдущего поколения, он потребует, чтобы эти устройства использовали механизмы RTS/CTS или CTS2Self при каждой передаче данных. Эта функция также поддерживает все стандартные режимы защиты 802.11n, включая MIMO.

Параметр RTS/CTS обеспечивает улучшенное покрытие, но снижает пропускную способность сети по сравнению с параметром CTS2Self, поскольку параметр RTS/CTS требует подтверждения от принимающего устройства. Чтобы использовать функцию RTS/CTS, оставьте значение по умолчанию, **RTS/CTS**. Параметр None (Нет) может вызвать конфликты между пакетами HT и пакетами предыдущего поколения. Чтобы использовать этот параметр, выберите **None** (Нет). Чтобы использовать параметр CTS2Self, выберите **CTS2Self**.

Percentage of maximal transmit power (Процентное отношение максимальной мощности передатчика) Этот параметр определяет процентное отношение максимальной мощности передатчика к мощности, разрешенной в данной местности. Например, если местное законодательство ограничивает мощность передатчика до 20 дБ, то установка процентного отношения 50 % ограничит максимальную мощность передачи до уровня 10 дБ. Выберите желаемое процентное соотношение: **12 %**, **25 %**, **50 %** или **100 %**. По умолчанию установлено значение **100 %**.

QoS Classification Type (Тип классификации QoS) Этот параметр устанавливает преобразование 802.1D или 802.1Q из поля IP DSCP/TOS в приоритеты WMM (Background (Фоновый), Best Effects (Оптимальные эффекты), Video (Видео), Voice (Голос)). Оставьте значение по умолчанию (**802.1D**) или выберите значение **802.1Q**, используемое некоторыми потоками IPTV.

Re-establish Ethernet connection when initiating wireless connection (Восстановление соединения Ethernet при установлении беспроводного соединения) Чтобы инициировать функцию обнаружения DHCP с устройства, расположенного за пределами зоны охвата моста, мост сбросит соединение Ethernet между мостом и устройством при каждом установлении беспроводного соединения. Чтобы отключить эту функцию, выберите **No** (Нет). В противном случае оставьте настройку по умолчанию – **Yes** (Да).

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

Administration (Администрирование) > Management (Управление)

На этом экране можно управлять специфическими функциями моста: доступ к веб-утилите, резервное копирование файла конфигурации и перезагрузка.



Управление

Доступ к мосту

Используйте пароль для защиты доступа к веб-утилите.

Bridge Password (Пароль моста) Введите новый пароль для доступа к мосту.

Re-enter to confirm (Повторный ввод для подтверждения) Повторно введите пароль для подтверждения.

Idle Timeout (Время ожидания действия) Авторизация пользователя аннулируется по истечении заданного времени бездействия. Диапазон действительных значений: от **60** до **3600** секунд. По умолчанию установлено значение **600**.

Доступ в Интернет

Access via Wireless (Доступ по беспроводной сети) Если мост используется в общедоступном домене, в котором предоставляется гостевой доступ к беспроводной сети, можно отключить беспроводной доступ к веб-утилите для настройки моста. Если эта функция отключена, доступ к маршрутизатору будет возможен только через проводное соединение. Для того чтобы разрешить беспроводный доступ к веб-утилите, оставьте значение по умолчанию **Enabled** (Включено); или выберите **Disabled** (Отключено) для блокировки беспроводного доступа к утилите.

Резервное копирование и восстановление

Backup (Резервное копирование) Для создания резервной копии настроек моста нажмите кнопку **Backup Configurations (Резервное копирование настроек)**. Затем следуйте инструкциям на экране.

Restore (Восстановление) Нажмите кнопку **Browse** (Обзор) и выберите файл конфигурации. Затем нажмите кнопку **Restore Configurations** (Восстановить настройки).

System Reboot (Перезагрузка системы)

Reboot (Перезагрузка) Для того чтобы перезагрузить или перезапустить мост, нажмите кнопку **Start to Reboot** (Начать перезагрузку).

Нажмите кнопку **Save Settings** (Сохранить настройки) для применения внесенных изменений или кнопку **Cancel Changes** (Отменить изменения) для их отмены.

Administration (Администрирование) > Factory Defaults (Заводские настройки)

На этом экране можно осуществить восстановление заводских настроек моста.

Заводские настройки

Restore All Settings (Восстановить все настройки) Для восстановления заводских настроек моста нажмите кнопку **Restore All Settings** (Восстановить все настройки). При восстановлении заводских настроек все сохраненные пользовательские настройки будут утеряны.



Administration (Администрирование) > Upgrade Firmware (Обновить прошивку)

На этом экране можно обновить прошивку моста. Не рекомендуется обновлять прошивку за исключением случаев, когда имеют место сбои в работе моста, или же новая версия прошивки содержит дополнительные функции, которые вы хотите использовать.



Для обновления прошивки необходимо сначала загрузить файл обновления моста с веб-сайта Linksys **www.linksys.com/support**.

Upgrade Firmware (Обновить прошивку)

Please select a file to upgrade the firmware (Выберите файл обновления прошивки) Нажмите кнопку **Browse** (Обзор) и выберите файл для обновления прошивки. Затем нажмите кнопку **Start to Upgrade** (Начать обновление) и следуйте инструкциям на экране.

Status (Состояние) > Bridge (Мост)

Отображается информация о текущем состоянии моста.



Bridge Information (Сведения о мосте)

Firmware Version (Версия прошивки) Отображается версия используемой прошивки.

Локальная сеть

Local MAC Address (Локальный MAC-адрес) Отображается MAC-адрес моста в локальной сети Ethernet.

IP Address (IP-адрес) Отображается IP-адрес моста, используемый в локальной сети Ethernet.

Subnet Mask (Маска подсети) Отображается установленная маска подсети вашей локальной сети.

Status (Состояние) > Wireless (Беспроводная сеть)

Отображается информация о состоянии вашей беспроводной сети.



Беспроводная сеть

Link Status (Состояние канала) Отображается состояние подключения к беспроводной сети.

MAC Address (MAC-адрес) Отображается MAC-адрес моста в локальной беспроводной сети.

Network Name (SSID) (Идентификатор сети SSID) Отображается имя или SSID беспроводной сети.

BSSID Отображается MAC-адрес в беспроводной сети подключенного маршрутизатора (или точки доступа).

Radio Band (Радиодиапазон) Отображается радиодиапазон беспроводной сети.

Channel Width (Ширина канала) Отображается ширина канала беспроводной сети (в МГц).

Wide Channel (Широкополосный канал) В зависимости от настроек канала сетевого маршрутизатора отображается широкополосный канал. Если для параметра Radio Band (Радиодиапазон) было выбрано значение Wide - 40MHz Channel (Широкополосный канал - 40 МГц), то это значение будет установлено для основного канала Wireless-N.

Standard Channel (Стандартный канал) Отображается настройка стандартного канала. Если для параметра Radio Band (Радиодиапазон) или Channel Width (Ширина канала) было выбрано значение Wide - 40MHz Channel (Широкий канал - 40 МГц), то задаваемый здесь стандартный канал будет установлен в качестве второстепенного для устройств Wireless-N.

Bit Rate (Скорость передачи данных) Отображается скорость передачи данных.

Signal (Сигнал) Отображается уровень сигнала в процентном соотношении. Значение 100 % указывает на самый высокий уровень сигнала; 0 % указывает на самый низкий уровень сигнала.

Security (Безопасность) Отображается метод обеспечения безопасности беспроводной сети.

Поиск и устранение неполадок

WES610N/WET610N

Компьютер или другое проводное Ethernet-устройство не может подключиться к беспроводному маршрутизатору.

1. Откройте веб-утилиту моста.
2. На экране *Basic Wireless Settings* (Основные настройки беспроводной сети) убедитесь в том, что сетевое имя (SSID) совпадает с именем беспроводной сети.
3. Убедитесь в том, что настройки безопасности сети (WPA, WPA2 или WEP) совпадают с настройками безопасности вашей беспроводной сети.

Необходимо изменить IP-адрес моста.

Если мост подключен к сети с DHCP-сервером (его роль, как правило, выполняет сетевой маршрутизатор), то свой IP-адрес он получит от DHCP-сервера. Если в сети нет DHCP-сервера, то мост использует статический IP-адрес по умолчанию: **169.254.1.250**.

Если требуется назначить мосту статический IP-адрес, выполните следующие действия:

1. Откройте веб-утилиту моста.
2. Перейдите на вкладку **Network Setup** (Настройка сети).
3. В выпадающем меню *Network Connection Type* (Тип сетевого подключения) выберите пункт **Static IP** (Статический IP-адрес).
4. Введите необходимую информацию в полях *Static IP Address* (Статический IP-адрес), *Subnet Mask* (Маска подсети) и *Default Gateway* (Основной шлюз).
5. Нажмите кнопку **Save Settings** (Сохранить настройки).

Компьютер или другое проводное Ethernet-устройство, подключенное к мосту, не может подключиться к другому беспроводному устройству (например, к компьютеру или принтеру).

Проверьте следующее:

- Убедитесь в том, что беспроводное устройство находится в той же беспроводной сети, что и компьютер или другое проводное Ethernet-устройство, подключенное к мосту.
- Убедитесь в том, что все устройства в беспроводной сети используют одинаковое сетевое имя (SSID).
- Убедитесь в том, что все устройства подключены к одной IP-сети с использованием совместимых IP-адресов.

Веб-утилита не принимает ваш пароль.

Проверьте следующее:

- Пароль вводится с учетом регистра клавиатуры. Проследите за тем, чтобы при вводе пароля учитывался регистр символов.
- Если вы забыли свой пароль, то можно восстановить заводские настройки моста, используемые по умолчанию.

 Нажмите и удерживайте кнопку **Reset** (Сброс) моста в течение примерно пяти секунд; будет восстановлен пароль, заданный производителем, – **admin**. Для всех прочих параметров моста также будут восстановлены заводские настройки. (Для входа в веб-утилиту введите **admin** в поле *Password* (Пароль).)

После проведенных в веб-утилите изменений новые значения параметров не отображаются на экране.

Нажмите кнопку **Refresh** (Обновить) в своем веб-браузере. Если новые настройки все еще не отображаются, выполните следующие действия:

1. Отключите адаптер питания от моста.
2. Подождите пять секунд и снова подключите адаптер питания к мосту.
3. Нажмите кнопку **Refresh** (Обновить) в своем веб-браузере.

ВЕБ
Если вы не нашли решения для своего вопроса, посетите веб-сайт Linksys по адресу **www.linksys.com**

Технические характеристики

WES610N

Модель	WES610N
Стандарты	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Индикаторы	Питание, Ethernet, Wi-Fi Protected Setup™, Беспроводное соединение, Подключение и активность каждого порта Ethernet
Порты	Ethernet (4), Питание
Кнопки	Reset (Сброс), Wi-Fi Protected Setup
Тип кабеля	CAT5e
Антенны	3 (внутренние)
Тип соединителя антенны	N/A
Съемные (да/нет)	Нет
Модуляция	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Мощность передатчика (эффективная изотропно-излучаемая мощность, EIRP) в дБм	802.11a: 15 дБм (номинал) при 54 Мбит/с 802.11b: 19 дБм (номинал) при 11 Мбит/с 802.11g: 16 дБм (номинал) при 54 Мбит/с 802.11n (2,4 ГГц): 18 дБм (номинал) при MCS15 802.11n (5 ГГц): 16 дБм (номинал) при MCS15
Чувствительность приемника	802.11a: -72 дБм (номинал) при 54 Мбит/с 802.11b: -85 дБм (номинал) при 11 Мбит/с 802.11g: -73 дБм (номинал) при 54 Мбит/с 802.11n (20 МГц): -75 дБм (номинал) при MCS15 802.11n (40 МГц): -69 дБм (номинал) при MCS15
Коэффициент усиления антенны в дБ относительно исзотропной антенны	1
Безопасность беспроводной сети	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Разрядность ключа безопасности	До 128 битов

Физические характеристики

Размеры	6,97 x 5,04 x 2,68" (177 x 128 x 68 мм)
Масса	295 г
Сертификация	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Питание	12 В, 1 А
Рабочая температура	От 0 до +40 °C
Температура хранения	От -20 до 60 °C
Рабочая влажность	10–85 % (без конденсации)
Влажность хранения	5–90 % (без конденсации)

Технические характеристики могут быть изменены без предварительного уведомления.

WET610N

Модель	WET610N
Стандарты	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Индикаторы	Питание, Ethernet, Wi-Fi Protected Setup™, Беспроводное соединение
Порты	Ethernet, Питание
Кнопки	Reset (Сброс), Wi-Fi Protected Setup
Тип кабеля	CAT5e
Антенны	3 (внутренние)
Тип соединителя антенны	N/A
Съемные (да/нет)	Нет
Модуляция	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Мощность передатчика (эффективная изотропно-излучаемая мощность, EIRP) в дБм	802.11a: 15 дБм (номинал) при в дБм 54 Мбит/с 802.11b: 18 дБм (номинал) при 11 Мбит/с 802.11g: 16 дБм (номинал) при 54 Мбит/с 802.11n: 12 дБм (номинал) при 130 Мбит/с (HT20), 270 Мбит/с (HT40)
Чувствительность приемника	802.11a: -72 дБм (номинал) при 54 Мбит/с 802.11b: -85 дБм (номинал) при 11 Мбит/с 802.11g: -73 дБм (номинал) при 54 Мбит/с 802.11n: -70 дБм (номинал) при MCS15/2,4 ГГц, -69 дБм (номинал) при MCS15/5,0 ГГц
Коэффициент усиления антенны в дБ относительно исзотропной антенны	1
Безопасность беспроводной сети	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Разрядность ключа безопасности	До 128 битов

Физические характеристики

Размеры:	5,71 x 4,17 x 2,05" (145 x 106 x 52 мм)
Масса	159 г
Сертификация	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Питание	12 В, 1 А
Рабочая температура	От 0 до +40 °C
Температура хранения	От -20 до 60 °C
Рабочая влажность	10–85 % (без конденсации)
Влажность хранения	5–90 % (без конденсации)

Технические характеристики могут быть изменены без предварительного уведомления.

Linksys.com/support

Cisco, логотип Cisco и Linksys являются товарными знаками или зарегистрированными товарными знаками Cisco и/или ее филиалов в США и других странах.
Список товарных знаков Cisco см. по адресу: www.cisco.com/go/trademarks. Все прочие товарные знаки, упомянутые в настоящем документе, являются собственностью соответствующих владельцев.

© Cisco и/или ее филиалы, 2011. Все права защищены.

3425-01249



Användarhandbok

Linksys WET610N/WES610N | Wireless-N-brygga med dualband

Innehåll

Produktöversikt

Lysdiodpaneler 2
Portpanelen 3

Checklista för trådlös säkerhet

Ändra standardnamn eller SSID för det trådlösa nätverket 4
Ändra standardlösenord 4
Aktivera MAC-adressfiltrering 4
Aktivera kryptering 4

Allmänna riktlinjer för nätverkssäkerhet 4
Ytterligare säkerhetstips 5

Avancerad konfiguration

Öppna det webbläsarbaserade verktyget 6
Setup (Konfiguration) > Basic Setup (Grundläggande inställningar) 7
Language (Språk) 7
Network Setup (Nätverksinställningar) 7

Wireless (Trådlöst) > Basic Wireless Settings (Grundläggande trådlösa inställningar). 7
Basic Wireless Settings (Grundläggande trådlösa inställningar) 8
Wireless Security (Trådlös säkerhet) 8
Wi-Fi Protected Setup 9

Wireless (Trådlöst) > Wireless Network Site Survey (Översikt över trådlös nätverksplats) 10
Wireless Network Site Survey (Översikt över trådlös nätverksplats) 10

Wireless (Trådlöst) > WMM® 11
WMM 12

Wireless (Trådlöst) > Advanced Wireless Settings (Avancerade trådlösa inställningar) 13
Advanced Wireless (Avancerade trådlösa inställningar) 14

Administration > Management (Hantering). 14
Management (Hantering) 15

Administration > Factory Defaults (Fabriksinställningar). 15
Factory Defaults (Fabriksinställningar) 15

Administration > Upgrade firmware (Uppgradera fast programvara) 15
Upgrade Firmware (Uppgradera fast programvara) 16

Status > Bridge (Brygga) 16
Information om bryggan 16
Lokalt nätverk 16

Status > Wireless (Trådlöst) 16
Trådlöst 16

Felsökning

WES610N/WET610N 17

Specifikationer

WES610N 18
WET610N 19

Produktöversikt

Tack för att du valde Linksys Wireless-N-brygga med dualband! Med den här bryggan kan du ansluta vilken trådbunden Ethernet-enhet som helst till det trådlösa nätverket. Bryggan bygger på dualband Wireless-N vilket innebär att den är kompatibel med vilken Wireless-N-, -G-, -A- eller -B-router som helst, eller med en åtkomstpunkt. Följ anvisningarna i CD-mappen när du installerar första gången. Använd det praktiska webbläsarbaserade verktyget om du vill konfigurera avancerade inställningar.

Lysdiodpaneler



WES610N WET610N

Wireless (Trådlöst, blå) Lysdioden för trådlöst nätverk tänds när det finns en trådlös anslutning. Lysdioden blinkar när bryggan aktivt skickar ut eller tar emot data över det trådlösa nätverket.

Knappen för Wi-Fi Protected Setup Om routern kan hantera Wi-Fi Protected Setup och använder WPA- eller WPA2-säkerhet kan du använda Wi-Fi Protected Setup för att automatiskt ansluta bryggan. Mer information om hur du använder Wi-Fi Protected Setup hittar du under ”Wireless (Trådlöst) > Basic Wireless Settings (Grundläggande trådlösa inställningar)” på sidan 7.

Lysdioden Wi-Fi Protected Setup (blå/orange) Lysdioden blinkar blått i två minuter vid konfigureringen med Wi-Fi Protected Setup. Den lyser blått när trådlös säkerhet aktiveras. Om det uppstår ett fel under konfigureringsprocessen med Wi-Fi Protected Setup lyser lysdioden orange. Kontrollera att nätverksroutern hanterar Wi-Fi Protected Setup. Vänta till lysdioden är släckt och försök sedan igen.

Ethernet (blå) Ethernet-lysdioden tänds när det finns en trådbunden anslutning. Lysdioden blinkar när bryggan aktivt skickar ut eller tar emot data genom Ethernet-porten/-portarna.

Power (Ström, blå) Strömlysdioden tänds när bryggan är påslagen.

Portpanelen



WES610N WET610N

Ethernet Ethernet-porten/-portarna ansluter bryggan till datorn eller till en annan Ethernet-nätverksenhet. WES610N har fyra portar, medan WET610N har en port.

Reset (Återställ) Du kan återställa bryggan till fabriksinställningarna på två sätt. Antingen håller du in knappen Reset (Återställ) i cirka fem sekunder eller så återställer du inställningarna från Administration > Factory Defaults (Fabriksinställningar) i bryggans webbaserade verktyg. WES610N har en återställningsknapp på undersidan, och på WET610N finns återställningsknappen på portpanelen bak.

Power (Ström) Strömporten ansluter bryggan till den medföljande strömadaptern.

Checklista för trådlös säkerhet

Trådlösa nätverk är praktiska och enkla att installera. Därför går allt fler hem med snabba Internet-anslutningar över till dem. Eftersom trådlösa nätverk arbetar genom att sända information via radiovågor riskerar de att i större utsträckning drabbas av intrång än traditionella trådbundna nätverk. Precis som signalerna från dina mobiltelefoner eller trådlösa telefoner, kan även signalerna från det trådlösa nätverket fångas upp. Eftersom du inte fysiskt kan förhindra att andra ansluter till det trådlösa nätverket måste du vidta några ytterligare steg för att hålla nätverket säkert.

Ändra standardnamn eller SSID för det trådlösa nätverket

Trådlösa enheter har ett standardnamn för nätverket eller SSID (Service Set Identifier) som anges på fabriken. Detta är det trådlösa nätverkets namn, som kan bestå av högst 32 tecken. Linksys trådlösa produkter använder **linksys** som standardnamn för trådlösa nätverk. Du bör ändra standardnamnet till något eget, så att ditt trådlösa nätverk kan särskiljas från eventuella andra trådlösa nätverk i din omgivning. Undvik dock att använda personlig information, t.ex. ditt personnummer, eftersom denna information eventuellt kan ses av andra som söker efter trådlösa nätverk.

Ändra standardlösenord

För trådlösa produkter, t.ex. åtkomstpunkter och routrar, får du ange ett lösenord när du vill ändra deras inställningar. Dessa enheter har ett standardlösenord som anges på fabriken. Routerns standardlösenord är **admin**. Hackare känner till dessa standardlösenord och kan försöka använda dem för att få tillgång till din trådlösa enhet och ändra dina nätverksinställningar. För att förhindra sådana obehöriga ändringar kan du ändra lösenordet till något som är svårt att gissa.

Aktivera MAC-adressfiltrering

Linksys routrar har funktioner för filtrering av MAC-adresser (Media Access Control). MAC-adressen är en unik serie nummer och bokstäver som tilldelas alla nätverksenheter. Om du aktiverar MAC-adressfiltreringen är det bara trådlösa enheter med angivna MAC-adresser som kommer åt ditt trådlösa nätverk. Exempel: du kan ange MAC-adressen för varje dator i hemmet så att bara de datorerna får tillgång till ditt trådlösa nätverk.

Aktivera kryptering

Kryptering skyddar de data som överförs över ett trådlöst nätverk. WPA/WPA2 (Wi-Fi Protected Access) och WEP (Wired Equivalent Privacy) erbjuder olika nivåer av säkerhet för trådlös kommunikation.

Ett nätverk som krypterats med WPA/WPA2 är mer säkert än ett nätverk som krypterats med WEP, eftersom WPA/WPA2 använder dynamisk nyckelkryptering. För att skydda den information som överförs via radiovågor bör du aktivera den högsta krypteringsnivå som stöds av din nätverksutrustning.

WEP är en äldre krypteringsstandard och är kanske det enda alternativ som kan användas för vissa äldre enheter som inte hanterar WPA.

Allmänna riktlinjer för nätverkssäkerhet

Trådlös nätverkssäkerhet är oduglig om det underliggande nätverket inte är säkert.

- Lösenordsskydda alla datorer på nätverket och ange separata lösenord för känsliga filer.
- Ändra lösenord med jämna mellanrum.
- Installera antivirusprogram och brandväggsprogramvara.
- Avaktivera fildelning (peer-to-peer). Det kan hända att vissa program aktiverar fildelning utan att du får godkänna eller känner till det.

Ytterligare säkerhetstips

- Håll trådlösa routrar, åtkomstpunkter och gateways borta från ytterväggar och fönster.
- Stäng av trådlösa routrar, åtkomstpunkter och gateways när de inte används (på natten och under semestrar).
- Använd starka lösenordsfraser som består av minst åtta tecken. Kombinera bokstäver och siffror för att undvika vanliga ord som kan hittas i lexikon.

Avancerad konfiguration

Bryggan är klar att användas när du har ställt in den enligt anvisningarna i CD-mappen. Om du vill ändra de avancerade inställningarna använder du bryggans webbläsarbaserade verktyg. I det här kapitlet beskrivs de olika webbsidorna i verktyget och nyckelfunktionerna på alla webbsidorna. Du kommer åt verktyget genom webbläsaren på en dator som är ansluten till bryggan.

Det webbläsarbaserade verktyget innehåller följande flikar: Setup (Konfiguration), Wireless (Trådlöst), Administration och Status. När du klickar på huvudflikarna visas ytterligare flikar.

Öppna det webbläsarbaserade verktyget

Du kommer åt det webbläsarbaserade verktyget med en webbläsare.

Om bryggan är ansluten till ett nätverk med DHCP-server (vanligtvis nätverksroutern) erhåller bryggan en IP-adress från DHCP-servern. Om det inte finns någon DHCP-server tillämpar bryggan den statiska, standardinställda IP-adressen **169.254.1.250**. (Om du ställer in en statisk permanent IP-adress på bryggan med hjälp av det webbläsarbaserade verktyget, anger du istället den statiska IP-adressen.)

OBS!
Bryggans IP-adress hittar du i routerns DHCP-klienttabell. (Se dokumentationen som följde med routern.)

Om du inte hittar bryggans IP-adress kan du återställa bryggan. Tryck bara på knappen **Reset** (Återställ) på själva bryggan i ungefär fem sekunder med hjälp av ett uträtat gem eller liknande. Då återställs bryggan till fabriksinställningarna. Du uppmanas att ange en IP-adress från DHCP-servern för bryggan (vanligen nätverksroutern). Om det inte finns någon DHCP-server använder bryggan den standardinställda, statiska IP-adressen **169.254.1.250**, tills en DHCP-server upptäcks och en dynamisk IP-adress kan tilldelas.

Om bryggan inte är ansluten till en router och fabriksinställningarna tillämpas, kan du ansluta bryggan till en dator med en Ethernet-anslutning om du vill komma åt det webbaserade- verktyget. Du måste konfigurera Ethernet-anslutningen i datorn med en statisk IP-adress och en nätmask.

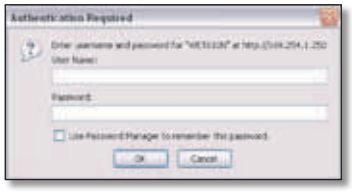
Ethernet-adapterns IP-adress ska vara specifik.

1. I fältet *IP address* (IP-adress) anger du **169.254.x.y** (x ska ersättas med ett tal mellan 1 och 254, och y ska ersättas med ett tal mellan 0 och 255).
2. I fältet *Subnet mask* (Nätmask) anger du **255.255.0.0**.

OBS!
Anvisningarna för hur du tilldelar en statisk IP-adress till Ethernet-adaptern i datorn varierar beroende på vilket operativsystem du har. Du hittar mer information i hjälpdokumentationen för ditt operativsystem.

Starta webbläsaren när Ethernet-adaptern har tilldelats en statisk IP-adress. Ange adapterns IP-adress (standardinställningen är **169.254.1.250**) i fältet *Address* (Adress). Tryck på **Enter**.

Nu öppnas en dialogruta där du ombeds att ange ditt lösenord. (Exemplet här är från Windows XP, men liknande dialogrutor visas i andra operativsystem.) Låt fältet *Användarnamn* vara tomt. Ange lösenordet som du skapade under installationen. Om du inte skapat ett nytt lösenord kan du använda standardlösenordet **admin**. (Du kan ställa in ett nytt lösenord på skärmen *Administration* > *Management* (Hantering).) Välj **OK** för att fortsätta.



OBS!
Om dialogrutan för att ange lösenordet inte visas kan du vänta i två minuter och försöka igen.

Setup (Konfiguration) > Basic Setup (Grundläggande inställningar)

Den första skärmen som visas är *Basic Setup* (Grundläggande inställningar). Här kan du ändra språk för det webbläsarbaserade verktyget, eller bryggans trådanslutna, Ethernet-inställningar.





Language (Språk)

Language (Språk) Med den här inställningen anger du vilket språk som ska visas i det webbläsarbaserade verktyget. Välj önskat språk i listrutan.

Network Setup (Nätverksinställningar)

I det här avsnittet avgörs om bryggans IP-adress kan hämtas automatiskt från en DHCP-server, till exempel nätverksroutern (Automatic Configuration [Automatisk konfiguration] – DHCP), eller om den måste anges manuellt (Static IP [Statisk IP-adress]).

Bridge IP (Bryggans IP) Om nätverket har en DHCP-server (nätverksroutern) som tilldelar IP-adresser till dina nätverksenheter, behåller du bara standardinställningen **Automatic Configuration – DHCP** (Automatisk konfiguration – DHCP). Du uppmanas att ange en IP-adress från DHCP-servern för bryggan (vanligen nätverksroutern). Om det inte finns någon DHCP-server använder bryggan den standardinställda, statiska IP-adressen **169.254.1.250**, tills en DHCP-server upptäcks och en dynamisk IP-adress kan tilldelas.

Om du vill ange en permanent statisk IP-adress för bryggan väljer du **Static IP** (Statisk IP).

Fyll i följande fält om du väljer Static IP (Statisk IP):

- **Static IP Address** (Statisk IP-adress) Ange en unik IP-adress som tillämpas för att komma åt det webbläsarbaserade verktyget.
- **Subnet Mask** (Nätmask) Ange nätmasken för det trådanslutna nätverket.
- **Default Gateway** (Standardgateway) Ange IP-adressen för nätverkets standardgateway (i de flesta fall är det här din router).

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Wireless (Trådlöst) > Basic Wireless Settings (Grundläggande trådlösa inställningar)

På skärmen *Basic Wireless Settings* (Grundläggande trådlösa inställningar) konfigurerar du bryggans grundläggande trådlösa inställningar och säkerhetsinställningar.

Du kan konfigurera bryggans inställningar på två sätt – manuellt eller med Wi-Fi Protected Setup. Wi-Fi Protected Setup är en funktion som gör det enkelt att konfigurera det trådlösa nätverket. Om nätverksroutern hanterar Wi-Fi Protected Setup och tillämpar WPA- eller WPA2-säkerhet, kan du ansluta bryggan automatiskt med hjälp av Wi-Fi Protected Setup.

Configuration View (Konfigurationsvy) Om du vill konfigurera det trådlösa nätverket manuellt väljer du **Manual** (Manuellt). Se avsnittet **Basic Wireless Settings** (Grundläggande trådlösa inställningar), **sida 8**. Om du vill använda Wi-Fi Protected Setup väljer du **Wi-Fi Protected Setup**. Se avsnittet **Wi-Fi Protected Setup**, **sida 9**.

Basic Wireless Settings (Grundläggande trådlösa inställningar)



Network Name (SSID) (Nätverksnamn [SSID]) Det här är nätverksnamnet som delas av alla enheter i ett trådlöst nätverk. Nätverksnamnet måste vara det samma för alla enheterna i det trådlösa nätverket. Det är skiftlägeskänsligt och får inte överstiga 32 tecken (du kan använda valfria tangenter på tangentbordet). Kontrollera att den här inställningen stämmer överens med inställningen för den trådlösa routern eller åtkomstpunkten. Av säkerhetsskäl bör du ändra standardnätverksnamnet (**linksys**) till ett eget namn.

Wireless Security (Trådlös säkerhet)

Bryggan kan hantera följande trådlösa säkerhetsalternativ: WPA Personal, WPA2 Personal och WEP. WPA (Wi-Fi Protected Access) och WPA2 är båda bättre säkerhetsmetoder än WEP (Wired Equivalent Privacy). Mer information om trådlös säkerhet hittar du i avsnittet "Checklista för trådlös säkerhet", sida 4.

Security Mode (Säkerhetsläge)

Välj rätt säkerhetsmetod för ditt trådlösa nätverk. Om du inte vill använda trådlös säkerhet behåller du bara standardinställningen **Disabled** (Avaktiverad).

OBS!
Kom ihåg att alla enheter i ditt trådlösa nätverk MÅSTE ha samma säkerhetsmetod och lösenordsfras/nyckel, annars kan de trådlösa enheterna inte kommunicera med varandra.

WPA Personal

WPA är en mer kraftfull säkerhetsstandard än WEP-kryptering.



Encryption (Kryptering) WPA hanterar TKIP-kryptering med dynamiska krypteringsnycklar.

Passphrase (Lösenordsfras) Ange nyckeln som delas av bryggan och den trådlösa routern eller åtkomstpunkten. Den ska bestå av 8–63 tecken.

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

WPA2 Personal

WPA2 är en mer avancerad, säkrare version av WPA.



Encryption (Kryptering) WPA2 hanterar två krypteringsmetoder, TKIP och AES, med dynamiska krypteringsnycklar. Välj krypteringsmetod: **AES** eller **TKIP eller AES**. Det standardinställda alternativet är **AES**.

Passphrase (Lösenordsfras) Ange nyckeln som delas av bryggan och den trådlösa routern eller åtkomstpunkten. Den ska bestå av 8–63 tecken.

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

WEP

WEP är en enkel krypteringsmetod som inte är lika säker som WPA eller WPA2.



Encryption (Kryptering) Välj nivå för WEP-kryptering: **40/64 bits (10 hex digits)** (40/60 bitar, 10 hexadecimala siffror) eller **104/128 bits (26 hex digits)** (104/128 bitar, 26 hexadecimala siffror). Standardinställningen är **40/64 bits (10 hex digits)** (40/64 bitar, 10 hexadecimala siffror).

Key 1 (Nyckel 1) Ange nätverkets WEP-nyckel.

Tx Key (TX-nyckel) **Key 1** (Nyckel 1) är sändningsnyckeln som tillämpas av bryggan.

Authentication (Autentisering) Standardinställningen är **Auto** (Automatiskt), vilket innebär att autentisering av typen Open System (Öppet system) eller Shared Key (Delad nyckel) kan användas. Välj **Open** (Öppen) om du vill tillämpa autentisering av typen Open System (Öppet system). Avsändaren och mottagaren använder ingen WEP-nyckel för autentisering. Välj **Shared** (Delad) om du vill tillämpa autentisering med delad nyckel. Avsändaren och mottagaren använder WEP-nyckel för autentisering.

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Wi-Fi Protected Setup

Det finns två metoder tillgängliga. Välj rätt metod för den router du använder.





Metod 1

Använd den här metoden om routern har en Wi-Fi Protected Setup-knapp.

1. Klicka eller tryck på **Wi-Fi Protected Setup**-knappen på routern.
2. Klicka på knappen **Wi-Fi Protected Setup** på bryggans *Wi-Fi Protected Setup*-skärm inom två minuter.
3. Klicka på **Close** (Stäng) när bryggan har konfigurerats.

På skärmen *Wi-Fi Protected Setup* visas länkstatus, nätverksnamn (SSID) och säkerhetsmetod.

Metod 2

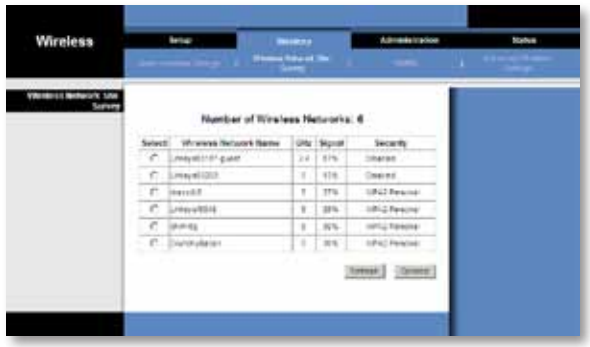
Använd den här metoden om routern kräver att du anger bryggans PIN-kod.

1. På **routerns** skärm för *Wi-Fi Protected Setup* anger du PIN-koden på **bryggans** *Wi-Fi Protected Setup*-skärm. Klicka sedan på **Register** (Registrera) eller annan lämplig knapp. (Den finns även på etiketten på undersidan av bryggan.)
2. På **bryggans skärm för** *Wi-Fi Protected Setup* klickar du på **OK**.
3. Klicka på **Close** (Stäng) när bryggan har konfigurerats.

På skärmen *Wi-Fi Protected Setup* visas länkstatus, nätverksnamn (SSID) och säkerhetsmetod.

Wireless (Trådlöst) > Wireless Network Site Survey (Översikt över trådlös nätverksplats)

Klicka på fliken **Wireless Network Site Survey** (Översikt över trådlös nätverksplats) om du vill starta översikten. På skärmen *Wireless Network Site Survey* (Översikt över trådlös nätverksplats) anges de trådlösa nätverk som bryggan har upptäckt.



Wireless Network Site Survey (Översikt över trådlös nätverksplats)

Number of Wireless Networks (Antal trådlösa nätverk) Antalet trådlösa nätverk som bryggan har upptäckt.

Select (Välj) Anslut till ett trådlöst nätverk genom att klicka på **Select** (Välj). Klicka sedan på **Connect** (Anslut).

Wireless Network Name (Trådlöst nätverksnamn) Nätverksnamnet eller SSID för det trådlösa nätverket visas.

GHz Det trådlösa nätverkets radioband visas.

Signal Den procentuella signalstyrkan visas. Den starkaste signalstyrkan är 100 %, medan 0 % är den svagaste.

Security (Säkerhet) Om nätverket hanterar Wi-Fi Protected Setup visas ikonen för Wi-Fi Protected Setup . Säkerhetsmetoden som tillämpas av det trådlösa nätverket visas.

Klicka på **Refresh** (Uppdatera) om du vill uppdatera uppgifterna på skärmen.

När du har valt ett nätverk klickar du på **Connect** (Anslut). Nu öppnas en ny skärm. Följ anvisningarna för nätverkets säkerhetsmetod.

WPA



Network Name (SSID) (Nätverksnamn [SSID]) Namnet som du gett nätverket visas automatiskt.

Security Mode (Säkerhetsläge) WPA Personal visas automatiskt.

Encryption (Kryptering) WPA hanterar TKIP-kryptering med dynamiska krypteringsnycklar.

Passphrase (Lösenordsfras) Ange nyckeln som delas av bryggan och den trådlösa routern eller åtkomstpunkten. Den ska bestå av 8–63 tecken.

Klicka på **Refresh** (Uppdatera) om du vill uppdatera uppgifterna på skärmen.

Klicka på **Connect** (Anslut) när du angett säkerhetsinställningarna.

WPA2



Network Name (SSID) (Nätverksnamn [SSID]) Namnet som du gett nätverket visas automatiskt.

Security Mode (Säkerhetsläge) WPA2 Personal visas automatiskt.

Encryption (Kryptering) WPA2 hanterar två krypteringsmetoder, TKIP och AES, med dynamiska krypteringsnycklar. Välj krypteringsmetod: **AES** eller **TKIP eller AES**.

Passphrase (Lösenordsfras) Ange nyckeln som delas av bryggan och den trådlösa routern eller åtkomstpunkten. Den ska bestå av 8–63 tecken.

Klicka på **Refresh** (Uppdatera) om du vill uppdatera uppgifterna på skärmen.

Klicka på **Connect** (Anslut) när du angett säkerhetsinställningarna.

WEP



Network Name (SSID) (Nätverksnamn [SSID]) Namnet som du gett nätverket visas automatiskt.

Security Mode (Säkerhetsläge) WEP visas automatiskt.

Encryption (Kryptering) Välj nivå för kryptering: **40/64 bits (10 hex digits)** (40/64 bitar, 10 hexadecimala siffror) eller **104/128 bits (26 hex digits)** (104/128 bitar, 26 hexadecimala siffror).

Key 1 (Nyckel 1) Ange nätverkets WEP-nyckel.

Tx Key (TX-nyckel) **Key 1** (Nyckel 1) är sändningsnyckeln som tillämpas av bryggan.

Authentication (Autentisering) Standardinställningen är **Auto** (Automatiskt), vilket innebär att autentisering av typen Open System (Öppet system) eller Shared Key (Delad nyckel) kan användas. Välj **Open** (Öppen) om du vill tillämpa autentisering av typen Open System (Öppet system). Avsändaren och mottagaren använder ingen WEP-nyckel för autentisering. Välj **Shared** (Delad) om du vill tillämpa autentisering med delad nyckel. Avsändaren och mottagaren använder WEP-nyckel för autentisering.

Klicka på **Refresh** (Uppdatera) om du vill uppdatera uppgifterna på skärmen.

Klicka på **Connect** (Anslut) när du angett säkerhetsinställningarna.

Wireless (Trådlöst) > WMM®

Konfigurera inställningarna för Wireless MultiMedia (WMM). WMM prioriterar paket beroende på deras respektive åtkomstläge (typ av trafik): Background (Bakgrund), Best Effort (Bästa försök), Video eller Voice (Röst). De här inställningarna får endast ändras av administratören eftersom felaktiga inställningar kan försämra den trådlösa funktionen.



OBS!
Inställningarna på skärmen *WMM* är endast avsedda för avancerade användare.

WMM

Access Mode (Åtkomstläge)

Du kan ange olika inställningar för de fyra tillgängliga åtkomstlägena. Välj ett läge som du vill konfigurera: **Background** (Bakgrund), **Best Effort** (Bästa försök), **Video** eller **Voice** (Röst). Följ anvisningarna för valt läge.

Background (Bakgrund)

Use Aggregation (Använd aggregering) Det här alternativet bestämmer om MAC-lagret (Media Access Control) ska installera en ADDBA-session (Add Block Acknowledgement) eller inte. Standardinställningen är **No** (Nej). Välj **Yes** (Ja) om du vill aktivera det här alternativet.

Accept Aggregation (Acceptera aggregering) Det här alternativet anger om MAC-lagret ska acceptera en ADDBA-begäran. Standardinställningen är **Yes** (Ja). Välj **No** (Nej) om du vill avaktivera det här alternativet.

Max. Number of Packets in Aggregation (Max. antal paket i aggregering) Det här alternativet bestämmer det maximala antalet paket (underramar) i aggregeringen. Omfånget är **0** till **7**. Standardinställningen är **7**.

Max. Aggregation Size (Max. aggregeringsstorlek) Det här alternativet anger den maximala storleken på aggregeringen (i byte). Omfånget är **0** till **16 000**. Standardinställningen är **12 000**.

Timeout Internal (Tidsgränsintervall) Det här alternativet bestämmer tidsgränsen inom vilken aggregeringen ska stängas med ett "stängningsvillkor" innan den stängs av timern. Omfånget är **0** till **100** ms. Standardinställningen är **3**.

Min. Size of Packet in Aggregation (Min. storlek på paket i aggregering) Det här alternativet bestämmer den minsta storleken (i byte) för paket som samlas i aggregeringen. Omfånget är **0** till **1 500**. Standardinställningen är **10**.

ADDBA Timeout (ADDBA-tidsgräns) Det här alternativet bestämmer tiden för när installationen av ADDBA ska slutföras, om inga ramar byts ut under den här tiden enligt ACK-överenskommelsen (Block Acknowledgement). Omfånget är **0** till **65 535** ms. Standardinställningen är **0**, vilket innebär att tidsgränsfunktionen är avaktiverad.

Aggregation Window Size (Storlek på aggregeringsfönster) Det här alternativet bestämmer det maximala antalet paket som kan överföras utan att ACK-meddelanden mottas. Omfånget är **0** till **64**. Standardinställningen är **64**.

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Best Effort (Bästa försök)

Use Aggregation (Använd aggregering) Det här alternativet bestämmer om MAC-lagret (Media Access Control) ska installera en ADDBA-session (Add Block Acknowledgement) eller inte. Standardinställningen är **Yes** (Ja). Välj **No** (Nej) om du vill avaktivera det här alternativet.

Accept Aggregation (Acceptera aggregering) Det här alternativet anger om MAC-lagret ska acceptera en ADDBA-begäran. Standardinställningen är **Yes** (Ja). Välj **No** (Nej) om du vill avaktivera det här alternativet.

Max. Number of Packets in Aggregation (Max. antal paket i aggregering) Det här alternativet bestämmer det maximala antalet paket (underramar) i aggregeringen. Omfånget är **0** till **10**. Standardinställningen är **10**.

Max. Aggregation Size (Max. aggregeringsstorlek) Det här alternativet anger den maximala storleken på aggregeringen (i byte). Omfånget är **0** till **20 000**. Standardinställningen är **16 000**.

Timeout Internal (Tidsgränsintervall) Det här alternativet bestämmer tidsgränsen inom vilken aggregeringen ska stängas med ett "stängningsvillkor" innan den stängs av timern. Omfånget är **0** till **100** ms. Standardinställningen är **3**.

Min. Size of Packet in Aggregation (Min. storlek på paket i aggregering) Det här alternativet bestämmer den minsta storleken (i byte) för paket som samlas i aggregeringen. Omfånget är **0** till **1 500**. Standardinställningen är **10**.

ADDBA Timeout (ADDBA-tidsgräns) Det här alternativet bestämmer tiden för när installationen av ADDBA ska slutföras, om inga ramar byts ut under den här tiden enligt ACK-överenskommelsen (Block Acknowledgement). Omfånget är **0** till **65 535** ms. Standardinställningen är **0**, vilket innebär att tidsgränsfunktionen är avaktiverad.

Aggregation Window Size (Storlek på aggregeringsfönster) Det här alternativet bestämmer det maximala antalet paket som kan överföras utan att ACK-meddelanden mottas. Omfånget är **0** till **64**. Standardinställningen är **64**.

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Video

Use Aggregation (Använd aggregering) Det här alternativet bestämmer om MAC-lagret (Media Access Control) ska installera en ADDBA-session (Add Block Acknowledgement) eller inte. Standardinställningen är **Yes** (Ja). Välj **No** (Nej) om du vill avaktivera det här alternativet.

Accept Aggregation (Acceptera aggregering) Det här alternativet anger om MAC-lagret ska acceptera en ADDBA-begäran. Standardinställningen är **Yes** (Ja). Välj **No** (Nej) om du vill avaktivera det här alternativet.

Max. Number of Packets in Aggregation (Max. antal paket i aggregering) Det här alternativet bestämmer det maximala antalet paket (underramar) i aggregeringen. Omfånget är **0** till **7**. Standardinställningen är **7**.

Max. Aggregation Size (Max. aggregeringsstorlek) Det här alternativet anger den maximala storleken på aggregeringen (i byte). Omfånget är **0** till **16 000**. Standardinställningen är **12 000**.

Timeout Internal (Tidsgränsintervall) Det här alternativet bestämmer tidsgränsen inom vilken aggregeringen ska stängas med ett "stängningsvillkor" innan den stängs av timern. Omfånget är **0** till **100** ms. Standardinställningen är **3**.

Min. Size of Packet in Aggregation (Min. storlek på paket i aggregering) Det här alternativet bestämmer den minsta storleken (i byte) för paket som samlas i aggregeringen. Omfånget är **0** till **1 500**. Standardinställningen är **10**.

ADDBA Timeout (ADDBA-tidsgräns) Det här alternativet bestämmer tiden för när installationen av ADDBA ska slutföras, om inga ramar byts ut under den här tiden enligt ACK-överenskommelsen (Block Acknowledgement). Omfånget är **0** till **65 535** ms. Standardinställningen är **0**, vilket innebär att tidsgränsfunktionen är avaktiverad.

Aggregation Window Size (Storlek på aggregeringsfönster) Det här alternativet bestämmer det maximala antalet paket som kan överföras utan att ACK-meddelanden mottas. Omfånget är **0** till **64**. Standardinställningen är **64**.

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Voice (Röst)

Use Aggregation (Använd aggregering) Det här alternativet bestämmer om MAC-lagret (Media Access Control) ska installera en ADDBA-session (Add Block Acknowledgement) eller inte. Standardinställningen är **Yes** (Ja). Välj **No** (Nej) om du vill avaktivera det här alternativet.

Accept Aggregation (Acceptera aggregering) Det här alternativet anger om MAC-lagret ska acceptera en ADDBA-begäran. Standardinställningen är **Yes** (Ja). Välj **No** (Nej) om du vill avaktivera det här alternativet.

Max. Number of Packets in Aggregation (Max. antal paket i aggregering) Det här alternativet bestämmer det maximala antalet paket (underramar) i aggregeringen. Omfånget är **0** till **2**. Standardinställningen är **2**.

Max. Aggregation Size (Max. aggregeringsstorlek) Det här alternativet anger den maximala storleken på aggregeringen (i byte). Omfånget är **0** till **16 000**. Standardinställningen är **10 000**.

Timeout Internal (Tidsgränsintervall) Det här alternativet bestämmer tidsgränsen inom vilken aggregeringen ska stängas med ett "stängningsvillkor" innan den stängs av timern. Omfånget är **0** till **100** ms. Standardinställningen är **10**.

Min. Size of Packet in Aggregation (Min. storlek på paket i aggregering) Det här alternativet bestämmer den minsta storleken (i byte) för paket som samlas i aggregeringen. Omfånget är **0** till **1 500**. Standardinställningen är **10**.

ADDBA Timeout (ADDBA-tidsgräns) Det här alternativet bestämmer tiden för när installationen av ADDBA ska slutföras, om inga ramar byts ut under den här tiden enligt ACK-överenskommelsen (Block Acknowledgement). Omfånget är **0** till **65 535** ms. Standardinställningen är **0**, vilket innebär att tidsgränsfunktionen är avaktiverad.

Aggregation Window Size (Storlek på aggregeringsfönster) Det här alternativet bestämmer det maximala antalet paket som kan överföras utan att ACK-meddelanden mottas. Omfånget är **0** till **64**. Standardinställningen är **64**.

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Wireless (Trådlöst) > Advanced Wireless Settings (Avancerade trådlösa inställningar)

Konfigurera bryggans avancerade trådlösa funktioner. De här inställningarna får endast ändras av administratören eftersom felaktiga inställningar kan försämra den trådlösa funktionen.



OBS!
Inställningarna på skärmen *Advanced Wireless Settings* (Avancerade trådlösa inställningar) är endast avsedda för avancerade användare.

Advanced Wireless (Avancerade trådlösa inställningar)

Use LDPC (Använd LDCP) LDCP (Low-Density Parity-Check Code) aktiverar eller avaktiverar felkorrigeringsläget för att minska risken för dataförlust i brusiga kanaler. Algoritmen för hastighetsanpassning avaktiverade automatiskt LDCP-kodningen vid arbete i höga PHY-hastigheter (över 162). Om du vill använda det avancerade felkorrigeringsschemat för LDCP låter du standardinställningen **Yes** (Ja) stå kvar. Annars väljer du **No** (Nej).

ERP Protection Type (ERP-skyddstyp) Det här alternativet konfigurerar skyddet av OFDM-paket trots att det finns 802.11b-stationer inom det trådlösa nätverket. När RTS/CTS- eller CTS2Self-paket skickas i 802.11b-hastigheter sänder bryggan information till det trådlösa nätverket om att OFDM-paket kommer att överföras och skyddar paketen i det trådlösa nätverket. RTS/CTS- och CTS2Self-paketen genererar pålägg som kan leda till lägre genomströmning.

RTS/CTS-alternativet ger bättre täckning men lägre genomströmning jämfört med CTS2Self. Det beror på att RTS/CTS-alternativet inbegriper godkännande från mottagarenheten. Om du vill använda RTS/CTS-alternativet behåller du standardinställningen **RTS/CTS**. Alternativet None (Inget) kan orsaka kollisioner mellan OFDM- och CCK-paket. Använd det här alternativet genom att välja **None** (Inget). Använd CTS2Self-alternativet genom att välja **CTS2Self**.

11n Protection Type (11n-skyddstyp) Det här alternativet konfigurerar skyddet från enheter med låg genomströmning i det trådlösa nätverket. Om den trådlösa routern (eller åtkomstpunkten) upptäcker en koppling till en äldre enhet med låg genomströmning kommer alla enheter med hög genomströmning att uppmanas använda RTS/CTS- eller CTS2Self-mekanismer före varje dataöverföring. Den här funktionen hanterar även alla 802.11n-standardskydd, inklusive MIMO.

RTS/CTS-alternativet ger bättre täckning men lägre genomströmning jämfört med CTS2Self. Det beror på att RTS/CTS-alternativet inbegriper godkännande från mottagarenheten. Om du vill använda RTS/CTS-alternativet behåller du standardinställningen **RTS/CTS**. Alternativet None (Inget) kan orsaka kollisioner mellan paket med hög genomströmning och äldra paket. Använd det här alternativet genom att välja **None** (Inget). Använd CTS2Self-alternativet genom att välja **CTS2Self**.

Percentage of maximal transmit power (Procent av maximal överföringseffekt) Det här alternativet bestämmer procentandelen av den maximala överföringseffekten i relation till domänrestriktionerna. Om domänrestriktionen till exempel tillåter överföringar på upp till 20 dB, kan den maximala överföringseffekten uppgå till 10 dB om procentandelen är inställd på 50 %. Välj önskad procentandel för överföring: **12 %**, **25 %**, **50 %** eller **100 %**. Standardinställningen är **100 %**.

QoS Classification Type (QoS-klassificeringstyp) Det här alternativet ändrar inställningarna för 802.1D- eller 802.1Q-mappning från IP DSCP/TOS-fältet till WMM-prioriteringar (Background (Bakgrund), Best Effects (Bästa försök), Video, Voice (Röst)). Behåll standardinställningen **802.1D** eller välj **802.1Q** som används av vissa IPTV-strömmar.

Re-establish Ethernet connection when initiating wireless connection (Återupprätta Ethernet-anslutningen när trådlösa anslutningar initieras) Bryggan återställer Ethernet-anslutningen mellan bryggan och respektive enhet varje gång en trådlös anslutning upprättas, så att DHCP-identifiering utlöses från enheten bakom bryggan. Avaktivera detta genom att välja **No** (Nej). Annars behåller du standardinställningen **Yes** (Ja).

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Administration > Management (Hantering)

På den här skärmen kan du hantera specifika funktioner i bryggan som att komma åt det webbaserade- verktyget, säkerhetskopiera konfigurationsfilen samt starta om.



Management (Hantering)

Åtkomst till brygga

Skydda åtkomsten till det webbläsarbaserade verktyget med ett lösenord.

Bridge Password (Bryggans lösenord) Ange ett nytt lösenord för bryggan.

Re-enter to confirm (Ange det på nytt för att bekräfta) Bekräfta genom att ange lösenordet igen.

Idle Timeout (Överskriden tidsgräns) Inloggningen avbryts efter en viss tids inaktivitet, som du själv kan ställa in. Omfånget är **60** till **3 600** sekunder. Standardinställningen är **600**.

Webbåtkomst

Access via Wireless (Åtkomst via trådlöst nätverk) Om du använder bryggan på en allmän plats där dina gäster har trådlös åtkomst, kan du förhindra åtkomst till bryggans webbläsarbaserade verktyg. Om du avaktiverar den här funktionen kommer du endast åt det webbläsarbaserade verktyget via en trådbunden anslutning. Behåll standardinställningen **Enabled** (Aktiverad) för att tillåta trådlös åtkomst till bryggans webbläsarbaserade verktyg, eller välj **Disabled** (Avaktiverad) om du vill blockera trådlös åtkomst till verktyget.

Säkerhetskopiera och återställa

Backup (Säkerhetskopiering) Om du vill säkerhetskopiera bryggans konfigurationsfil klickar du på **Backup Configurations** (Säkerhetskopiera konfigurationer). Följ sedan anvisningarna på skärmen.

Restore (Återställ) Klicka på **Browse** (Bläddra) och välj konfigurationsfil. Klicka sedan på **Restore Configurations** (Återställ konfigurationer).

Starta om systemet

Reboot (Starta om) Om du vill starta om bryggan klickar du bara på **Start to Reboot** (Starta omstart).

Klicka på **Save Settings** (Spara inställningar) så sparas dina ändringar, eller välj **Cancel Changes** (Avbryt ändringar) om du vill avbryta utan att spara ändringarna.

Administration > Factory Defaults (Fabriksinställningar)

På den här skärmen kan du återställa bryggans konfiguration till fabriksinställningarna.

Factory Defaults (Fabriksinställningar)

Restore All Settings (Återställ alla inställningar) Om du vill återställa bryggans inställningar till fabriksinställningarna klickar du på **Restore All Settings** (Återställ alla inställningar). De inställningar som du har gjort försvinner när standardinställningarna återställs.



Administration > Upgrade firmware (Uppgradera fast programvara)

På den här skärmen kan du uppgradera bryggans fasta programvara. Du bör endast uppgradera den fasta programvaran om du har problem med bryggan eller om den nya fasta programvaran innehåller en funktion som du vill använda.



Innan du uppgraderar den fasta programvaran hämtar du bryggans uppgraderingsfil för den fasta programvaran från Linksys webbplats: **www.Linksys.com/support**.

Upgrade Firmware (Uppgradera fast programvara)

Please select a file to upgrade the firmware (Välj en fil för att uppgradera den fasta programvaran) Klicka på **Browse** (Bläddra) och välj uppgraderingsfil för den fasta programvaran. Klicka sedan på **Start to Upgrade** (Påbörja uppgradering) och följ anvisningarna på skärmen.

Status > Bridge (Brygga)

Bryggans aktuella statusinformation visas.



Information om bryggan

Firmware Version (Version av fast programvara) Bryggans befintliga version av den fasta programvaran visas.

Lokalt nätverk

Local MAC Address (Lokal MAC-adress) Bryggans MAC-adress, såsom den visas i ditt lokala Ethernet-nätverk.

IP Address (IP-adress) Bryggans IP-adress, såsom den visas i ditt lokala Ethernet-nätverk.

Subnet Mask (Nätmask) Nätmasken som konfigurerats för ditt lokala nätverk visas.

Status > Wireless (Trådlöst)

Information om det trådlösa nätverket visas här.



Trådlöst

Link Status (Länkstatus) Det trådlösa nätverkets anslutningsstatus visas här.

MAC Address (MAC-adress) Bryggans MAC-adress, såsom den visas i det lokala trådlösa nätverket.

Network Name (SSID) (Nätverksnamn [SSID]) Det trådlösa nätverkets namn eller SSID visas här.

BSSID Den trådlösa MAC-adressen för den anslutna trådlösa routern (eller åtkomstpunkten) visas.

Radio Band (Radioband) Radiobandet för det trådlösa nätverket visas.

Channel Width (Kanalbredd) Kanalbredden för det trådlösa nätverket visas i MHz.

Wide Channel (Bred kanal) Beroende på kanalinställningarna för nätverksroutern visas Wide Channel (bred kanal). Om du har valt Wide – 40 MHz (Bred – 40 MHz) för routerns inställning för radioband eller kanalbredd blir detta din primära Wireless-N-kanal.

Standard Channel (Standardkanal) Inställningen för standardkanal visas. Om du har valt Wide – 40 MHz (Bred – 40 MHz) för routerns inställning för radioband eller kanalbredd blir standardkanalen en sekundär kanal för Wireless-N.

Bit Rate (Bithastighet) Dataöverföringshastigheten visas.

Signal Den procentuella signalstyrkan visas. Den starkaste signalstyrkan är 100 %, medan 0 % är den svagaste.

Security (Säkerhet) Säkerhetsmetoden för det trådlösa nätverket visas.

Felsökning

WES610N/WET610N

Datorn eller andra trådbundna Ethernet-enheter kan inte kommunicera med den trådlösa routern.

1. Öppna bryggans webbläsarbaserade verktyg.
2. Se till att nätverksnamnet (SSID) på skärmen *Basic Wireless Settings* (Grundläggande trådlösa inställningar) är detsamma som namnet på det trådlösa nätverket.
3. Kontrollera att säkerhetsinställningarna (WPA, WPA2 eller WEP) stämmer överens med säkerhetsinställningarna för det trådlösa nätverket.

Bryggans IP-adress måste ändras.

Om bryggan är ansluten till ett nätverk med en DHCP-server (vanligen nätverksroutern), hämtar bryggan en IP-adress från DHCP-servern. Om det inte finns någon DHCP-server tillämpar bryggan den statiska, standardinställda IP-adressen **169.254.1.250**.

Följ anvisningarna nedan om du vill att bryggan alltid ska använda en statisk IP-adress:

1. Öppna bryggans webbläsarbaserade verktyg.
2. Klicka på fliken **Network Setup** (Nätverksinställningar).
3. I listrutan *Network Connection Type* (Typ av nätverksanslutning) markerar du **Static IP** (Statisk IP).
4. Fyll i fälten *Static IP Address* (Statisk IP-adress), *Subnet Mask* (Nätmask) och *Default Gateway* (Standardgateway).
5. Klicka på **Save settings** (Spara inställningar).

Den dator som aktiverats av bryggan eller andra trådbundna Ethernet-enheter kan inte kommunicera med trådlösa enheter som aktiverats (exempelvis dator eller skrivare).

Kontrollera följande:

- Kontrollera att den trådlösa enhet som anslutits finns på samma trådlösa nätverk som den dator eller andra trådbundna Ethernet-enheter som är anslutna till bryggan.
- Kontrollera att samma nätverksnamn (SSID) används för samtliga enheter i det trådlösa nätverket.
- Kontrollera att alla enheter finns på samma IP-nätverk och använder kompatibla IP-adresser.

Lösenordet accepteras inte av det webbaserade verktyget.

Kontrollera följande:

- Lösenordet är skiftlägeskänsligt. Kontrollera att du skriver in lösenordet med de rätta stora/små bokstäverna.
- Om du glömmer bort ditt lösenord kan du återställa bryggan till fabriksinställningarna.

 Tryck på och håll ned knappen **Reset** (Återställ) på bryggan i cirka fem sekunder. Lösenordet återställs då till det fabriksinställda **admin**. Övriga inställningar för bryggan kommer också att återställas till fabriksinställningarna. (Om du vill öppna det webbaserade verktyget skriver du in **admin** i fältet *Password* [Lösenord].)

De nya inställningarna visas inte på skärmen när du ändrar inställningar med det webbaserade verktyget.

Klicka på **Refresh** (Uppdatera) i webbläsaren. Följ anvisningarna nedan om de nya inställningarna inte visas:

1. Koppla bort strömadaptern från bryggan.
2. Vänta fem sekunder och koppla därefter in strömadaptern i bryggan igen.
3. Klicka på **Refresh** (Uppdatera) i webbläsaren.

INFORMATION PÅ WEBBEN
Om du har frågor som inte tas upp här kan du gå till Linksys webbplats **Linksys.com/support**

Specifikationer

WES610N

Modell	WES610N
Standarder	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Lysdioder	Power (Ström), Ethernet, Wi-Fi Protected Setup™, Wireless (Trådlös anslutning), enskild Ethernet-anslutning och aktivitet
Portar	Ethernet (4), Power (Ström)
Knappar	Reset (Återställ), Wi-Fi Protected Setup
Kabeltyp	KAT 5e
Antenner	3 (interna)
Antennanslutningstyp	Ej tillämpligt
Löstagbar (Ja/Nej)	Nej
Moduleringar	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF-effekt (EIRP) i dBm	802.11a: 15 dBm (normalt) vid 54 Mbit/s 802.11b: 19 dBm (normalt) vid 11 Mbit/s 802.11g: 16 dBm (normalt) vid 54 Mbit/s 802.11n (2,4 GHz): 18 dBm (normalt) vid MCS15 802.11n (5 GHz): 16 dBm (normalt) vid MCS15
Mottagningskänslighet	802.11a: -72 dBm (normalt) vid 54 Mbit/s 802.11b: -85 dBm (normalt) vid 11 Mbit/s 802.11g: -73 dBm (normalt) vid 54 Mbit/s 802.11n (20 MHz): -75 dBm (normalt) vid MCS15 802.11n (40 MHz): -69 dBm (normalt) vid MCS15
Antennförstärkning i dBi	1
Trådlös säkerhet	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Säkerhetsnyckelbitar	Upp till 128-bitarskryptering

Miljö

Storlek	177 x 128 x 68 mm (6,97 x 5,04 x 2,68 tum)
Vikt	295 g
Certifiering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Ström	12 V, 1A
Temperatur vid användning	0 till 40 °C (32 till 104 °F)
Förvaringstemperatur	-20 till 60 °C (-4 till 140 °F)
Luftfuktighet vid användning	10 till 85 % ej kondenserande
Luftfuktighet vid förvaring	5 till 90 % ej kondenserande

Specifikationerna kan ändras utan föregående meddelande.

WET610N

Modell	WET610N
Standarder	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Lysdioder	Power (Ström), Ethernet, Wi-Fi Protected Setup™, Wireless (Trådlös anslutning)
Portar	Ethernet, Power (Ström)
Knappar	Reset (Återställ), Wi-Fi Protected Setup
Kabeltyp	KAT 5e
Antenner	3 (interna)
Antennanslutningstyp	Ej tillämpligt
Löstagbar (Ja/Nej)	Nej
Moduleringar	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF-effekt (EIRP) i dBm	802.11a: 15 dBm (normalt) vid 54 Mbit/s 802.11b: 18 dBm (normalt) vid 11 Mbit/s 802.11g: 16 dBm (normalt) vid 54 Mbit/s 802.11n: 12 dBm (normalt) vid 130 Mbit/s (HT20), 270 Mbit/s (HT40)
Mottagningskänslighet	802.11a: -72 dBm (normalt) vid 54 Mbit/s 802.11b: -85 dBm (normalt) vid 11 Mbit/s 802.11g: -73 dBm (normalt) vid 54 Mbit/s 802.11n: -70 dBm (normalt) vid MCS15/2,4 GHz, -69 dBm (normalt) vid MCS15/5,0 GHz
Antennförstärkning i dBi	1
Trådlös säkerhet	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Säkerhetsnyckelbitar	Upp till 128-bitarskryptering

Miljö

Storlek	145 x 106 x 52 mm (5,71 x 4,17 x 2,05 tum)
Vikt	159 g
Certifiering	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Ström	12 V, 1A
Temperatur vid användning	0 till 40 °C (32 till 104 °F)
Förvaringstemperatur	-20 till 60 °C (-4 till 140 °F)
Luftfuktighet vid användning	10 till 85 % ej kondenserande
Luftfuktighet vid förvaring	5 till 90 % ej kondenserande

Specifikationerna kan ändras utan föregående meddelande.

Linksys.com/support

Cisco, Cisco-logotypen och Linksys är registrerade varumärken eller varumärken som tillhör Cisco och/eller dess samarbetspartner i USA och andra länder.
En lista över Ciscos varumärken finns på www.cisco.com/go/trademarks. Alla andra varumärken som nämns i det här dokumentet tillhör respektive ägare.

© 2011 Cisco och/eller dess samarbetspartner. Med ensamrätt.

3425-01249



Navodila za uporabo

Razvedrilni most Linksys WET610N/WES610N

N z dvema frekvenčnima pasovoma

Kazalo

Pregled izdelka

Plošča z indikatorji LED 2
Plošča z vrati 3

Varnostni seznam za zaščito brezžičnega omrežja

Spreminjanje privzetega imena ali SSID-ja brezžičnega omrežja 4
Spreminjanje privzetega gesla 4
Omogočanje filtriranja naslovov MAC 4
Omogočanje šifriranja 4

Splošne smernice za zaščito omrežja 4
Dodatni varnostni namigi 5

Dodatna konfiguracija

Dostop do pripomočka v brskalniku 6
Setup (Nastavitev) > Basic Setup (Osnovna nastavitev) 7
Language (Jezik) 7
Network Setup (Nastavitev omrežja) 7
Wireless (Brezžična povezava) > Basic Wireless Settings (Osnovne brezžične nastavitve) 7
Basic Wireless Settings (Osnovne brezžične nastavitve) 8
Wireless Security (Varnost brezžičnih omrežij) 8
Wi-Fi Protected Setup 9
Wireless (Brezžična povezava) > Wireless Network Site Survey (Pregled mest brezžičnega omrežja) 10
Wireless Network Site Survey (Pregled mest brezžičnega omrežja) 10
Wireless (Brezžična povezava) > WMM® 11
WMM 12
Wireless (Brezžična povezava) > Advanced Wireless Settings (Dodatne brezžične nastavitve) 13
Advanced Wireless (Dodatne nastavitve brezžične povezave) 14
Administration (Skrbništvo) > Management (Upravljanje) . . . 14
Management (Upravljanje) 14
Administration (Skrbništvo) > Factory Defaults (Tovarniško privzete vrednosti). 15
Factory Defaults (Tovarniško privzete vrednosti) 15
Administration (Skrbništvo) > Upgrade Firmware (Nadgradnja vgrajene programske opreme) 15
Upgrade Firmware (Nadgradnja vgrajene programske opreme) 15
Status (Stanje) > Bridge (Most) 16
Bridge Information (Informacije o mostu) 16
Local Network (Lokalno omrežje) 16
Status (Stanje) > Wireless (Brezžična povezava) 16
Wireless (Brezžična povezava) 16

Odpravljanje napak

WES610N/WET610N 17

Specifikacije

WES610N 18
WET610N 19

Pregled izdelka

Hvala, ker ste izbrali razvedrilni most Linksys N z dvema frekvenčnima pasovoma. Z mostom lahko katero koli žično ethernetno napravo povežete z brezžičnim omrežjem. Most temelji na tehnologiji Wireless-N z dvema frekvenčnima pasovoma, zato je združljiv z vsemi usmerjevalniki ali dostopnimi točkami Wireless-N, -G, -A ali -B. Pri prvi namestitvi sledite korakom v mapi na CD-ju. Za konfiguracijo naprednih nastavitev uporabite priročen pripomoček v brskalniku.

Plošča z indikatorji LED



WES610N WET610N

Brezžična povezava (modra) Indikator za brezžično povezavo sveti, ko je vzpostavljena brezžična povezava. Indikator utripa, ko most prek brezžičnega omrežja aktivno pošilja ali prejema podatke.

Gumb Wi-Fi Protected Setup Če usmerjevalnik podpira Wi-Fi Protected Setup in uporablja zaščito WPA ali WPA2, lahko most samodejno povežete s funkcijo Wi-Fi Protected Setup. Če želite uporabiti Wi-Fi Protected Setup, si oglejte razdelek »Wireless (Brezžična povezava) > Basic Wireless Settings (Osnovne brezžične nastavitve)« na strani 7.

Indikator Wi-Fi Protected Setup (modra/oranžna) Med postopkom nastavitve s funkcijo Wi-Fi Protected Setup indikator utripa modro. Ko je brezžična zaščita omogočena, sveti modro. Če pride med postopkom nastavitve s funkcijo Wi-Fi Protected Setup do napake, indikator sveti oranžno. Preverite, ali omrežni usmerjevalnik podpira Wi-Fi Protected Setup. Počakajte, da indikator ugasne in poskusite znova.

Ethernetna povezava (modra) Indikator za ethernetno povezavo sveti, ko je vzpostavljena žična povezava. Indikator utripa, ko most prek ethernetnih vrat aktivno pošilja ali prejema podatke.

Vklop/izklop (modra) Indikator za vklop/izklop sveti, ko je most vklopljen.

Plošča z vrati



WES610N WET610N

Ethernet Ethernetna vrata most povezujejo z računalnikom ali drugo ethernetno omrežno napravo. WES610N ima štiri vrata, WET610N pa ena.

Ponastavitev Most lahko na tovarniške nastavitve ponastavite na dva načina. Pritisnite in približno pet sekund držite gumb za ponastavitev ali pa privzete vrednosti obnovite na zaslonu Administration (Skrbništvo) > Factory Defaults (Tovarniško privzete vrednosti) v pripomočku mostu v brskalniku. WES610N ima gumb za nastavitev na spodnji strani, WET610N pa na plošči z vrati na zadnji strani.

Napajanje Prek priključka za napajanje je most priklopljen na priložen napajalnik.

Varnostni seznam za zaščito brezžičnega omrežja

Brezžična omrežja so priročna in preprosta za namestitev, zato so vedno bolj razširjena v domovih z dostopom do hitrega interneta. Brezžična omrežja pošiljajo podatke prek radijskih valov, zato so lahko bolj ranljiva od običajnih žičnih omrežij. Podobno kot pri mobilnih ali prenosnih telefonih lahko vsiljivci prestrežejo signale iz brezžičnega omrežja. Ker drugim ne morete fizično preprečiti, da bi se povezali z vašim brezžičnim omrežjem, morate za zaščito omrežja izvesti nekaj dodatnih ukrepov.

Spreminjanje privzetega imena ali SSID-ja brezžičnega omrežja

Brezžične naprave imajo privzeto ime brezžičnega omrežja ali identifikator nabora storitev (SSID), ki ga določi proizvajalec. To je ime brezžičnega omrežja, ki je lahko dolgo največ 32 znakov. Brezžični izdelki Linksys imajo za privzeto ime brezžičnega omrežja **linksys**. Ime brezžičnega omrežja spremenite v edinstven niz, s katerim boste vaše brezžično omrežje ločili od drugih, ki so lahko blizu vas. Za poimenovanje ne uporabljajte osebnih podatkov (na primer EMŠO), ker jih lahko vidijo vsi, ki iščejo brezžična omrežja.

Spreminjanje privzetega gesla

Če boste želeli spremeniti nastavitve dostopnih točk in usmerjevalnikov, boste morali vnesti geslo. Privzeto geslo za te naprave nastavi proizvajalec. Privzeto geslo za naprave Linksys je **admin**. Hekerji poznajo ta privzeta gesla in jih bodo poskušali uporabiti, da bi pridobili dostop do vaše brezžične naprave in spremenili omrežne nastavitve. Nepooblaščene spremembe preprečite tako, da geslo naprave spremenite v takega, da ga bo težko uganiti.

Omogočanje filtriranja naslovov MAC

Na usmerjevalnikih Linksys lahko omogočite filtriranje naslovov MAC (Media Access Control). Naslov MAC je edinstven niz številk in črk, dodeljen vsaki omrežni napravi. Ko je filtriranje naslovov MAC omogočeno, lahko do brezžičnega omrežja dostopajo le brezžične naprave z določenimi naslovi MAC. Navedete lahko na primer naslove MAC vseh domačih računalnikov, da imajo dostop do brezžičnega omrežja samo ti.

Omogočanje šifriranja

Šifriranje zaščiti podatke, oddane prek brezžičnega omrežja. Wi-Fi Protected Access (WPA/WPA2) in Wired Equivalent Privacy (WEP) ponujata različne ravni varnosti za brezžično komunikacijo.

Omrežje, šifrirano z načinom WPA/WPA2, je varnejše od omrežja, šifriranega z načinom WEP, ker WPA/WPA2 uporablja dinamično šifriranje ključa. Če želite zaščititi podatke, ki potujejo po zraku, omogočite najvišjo raven šifriranja, ki ga omogoča omrežje.

WEP je starejši način šifriranja in je morda edina razpoložljiva možnost za starejše naprave, ki ne podpirajo standarda WPA.

Splošne smernice za zaščito omrežja

Zaščita brezžičnega omrežja ni smiselna, če ni varno osnovno omrežje.

- Z geslom zaščitite vse računalnike v omrežju in še dodatno vse občutljive datoteke.
- Gesla redno spreminjajte.
- Namestite protivirusno programsko opremo in osebni požarni zid.
- Onemogočite izmenjavo datotek (med enakovrednimi računalniki). Nekateri programi lahko začnejo izmenjevati datoteke brez vaše privolitve in/ali vednosti.

Dodatni varnostni namigi

- Brezžične usmerjevalnike, dostopne točke ali prehode postavite stran od zunanjih zidov in oken.
- Ko brezžičnih usmerjevalnikov, dostopnih točk ali prehodov ne uporabljate (ponoči, med počitnicami), jih izklopite.
- Uporabljajte varna gesla, dolga vsaj osem znakov. Združujte črke in številke, da se izognete običajnim besedam, ki jih je mogoče poiskati v slovarju.

Dodatna konfiguracija

Po nastavitvi mostu z upoštevanjem korakov v mapi na CD-ju bo ta pripravljen za uporabo. Če pa želite spremeniti dodatne nastavitve, uporabite pripomoček mostu v brskalniku. V tem poglavju so opisane vse spletne strani pripomočka in ključne funkcije na vsaki strani. Do pripomočka lahko dostopate v spletnem brskalniku računalnika, ki je povezan z mostom.

Pripomoček v brskalniku ima te glavne zavihke: Setup (Nastavitev), Wireless (Brezžična povezava), Administration (Skrbništvo) in Status (Stanje). Ko kliknete enega od glavnih zavihkov, bodo na voljo še dodatni zavihki.

Dostop do pripomočka v brskalniku

Za dostop do pripomočka v brskalniku uporabite spletni brskalnik.

Če je most povezan z omrežjem, ki ima strežnik DHCP (običajni usmerjevalnik omrežja), bo most naslov IP pridobil pri strežniku DHCP. Če strežnika DHCP ni, bo most uporabil privzet statičen naslov IP **169.254.1.250**. (Če s pripomočkom v brskalniku mostu dodelite stalen statičen naslov IP, vnesite tega.)

OPOMBA
Če naslova IP mostu ne poznate, ga poiščite v tabeli odjemalcev DHCP usmerjevalnika. (Oglejte si dokumentacijo usmerjevalnika.)

Če naslova IP mostu ne morete najti, lahko most ponastavite; pritisnite in z zravnano sponko za papir približno pet sekund držite gumb za **ponastavitev** na mostu. Tako boste most ponastavili na tovarniško privzete vrednosti. Most bo od strežnika DHCP (običajno usmerjevalnik omrežja) zahteval naslov IP. Če strežnika DHCP ni, bo most uporabil privzet statičen naslov IP **169.254.1.250**, dokler ne zazna strežnika DHCP, ki mu dodeli dinamičen naslov IP.

Če most ni povezan z usmerjevalnikom in uporablja tovarniško privzete nastavitve, boste dostop do pripomočka v brskalniku omogočili tako, da računalnik z ethernetno povezavo povežete z mostom. Ethernetni povezavi računalnika boste morali dodeliti statičen naslov IP in masko podomrežja.

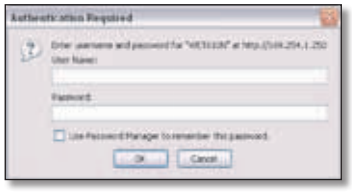
Naslov IP ethernetnega vmesnika morate nastaviti na določen naslov IP.

1. V polje *IP address* (Naslov IP) vnesite **169.254.x.y** (x zamenjajte s številko med 1 in 254, y pa s številko med 0 in 255).
2. V polje *Subnet mask* (Maska podomrežja) vnesite **255.255.0.0**.

OPOMBA
Postopek za dodelitev statičnega naslova IP ethernetnemu vmesniku v računalniku je odvisen od operacijskega sistema. Za navodila si oglejte dokumentacijo s pomočjo za operacijski sistem, ki ga uporabljate.

Ko ethernetnemu vmesniku dodelite statičen naslov IP, zaženite spletni brskalnik in v polje *Address* (Naslov) vnesite naslov IP vmesnika (privzeta vrednost je **169.254.1.250**). Pritisnite **Enter**.

Prikaže se zaslon, na katerem morate vnesti geslo. (Uporabniki, ki ne uporabljajo Windows XP, bodo videli podoben zaslon.) Polje *User name* (Uporabniško ime) pustite prazno. Vnesite geslo, ki ste ga ustvarili v čarovniku za namestitev. Če novega gesla niste ustvarili, uporabite privzeto geslo **admin**. (Novo geslo lahko nastavite na zaslonu *Administration* (Skrbništvo) > *Management* (Upravljanje).) Za nadaljevanje kliknite **OK** (V redu).



OPOMBA
Če se zaslon za vnos gesla ne prikaže, počakajte dve minuti in poskusite znova.

Setup (Nastavitev) > Basic Setup (Osnovna nastavitev)

Najprej se pojavi zaslon *Basic Setup* (Osnovna nastavitev). Na tem zaslonu lahko spremenite jezik pripomočka v brskalniku ali nastavitve žičnega ethernetnega omrežja mostu.





Language (Jezik)

Language (Jezik) Tukaj lahko nastavite jezik pripomočka v brskalniku. Želeni jezik izberite v spustnem meniju.

Network Setup (Nastavitev omrežja)

Ta razdelek določa, ali most naslov IP samodejno pridobi od strežnika DHCP, na primer omrežnega usmerjevalnika (Automatic Configuration - DHCP (Samodejna konfiguracija – DHCP)) ali pa ga nastavite ročno (Static IP (Statičen IP)).

Bridge IP (IP mostu) Če omrežnim napravam naslove IP dodeljuje strežnik DHCP, na primer omrežni usmerjevalnik, obdržite privzeto nastavitev **Automatic Configuration - DHCP** (Samodejna konfiguracija – DHCP). Most bo od strežnika DHCP (običajno usmerjevalnika omrežja) zahteval naslov IP. Če strežnika DHCP ni, bo most uporabil privzet statičen naslov IP **169.254.1.250**, dokler ne zazna strežnika DHCP, ki mu dodeli dinamičen naslov IP.

Če želite za most nastaviti trajen statičen naslov IP, izberite **Static IP** (Statičen IP).

Če izberete to možnost, izpolnite ta polja:

- **Static IP Address** (Statičen naslov IP) Vnesite edinstven naslov IP, ki se bo uporabljal za dostop do pripomočka v brskalniku.
- **Subnet Mask** (Maska podomrežja) Vnesite masko podomrežja žičnega omrežja.
- **Default Gateway** (Privzet prehod) Vnesite naslov IP privzetega prehoda omrežja (v večini primerov je to usmerjevalnik).

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Wireless (Brezžična povezava) > Basic Wireless Settings (Osnovne brezžične nastavitve)

Na zaslonu *Basic Wireless Settings* (Osnovne brezžične nastavitve) lahko konfigurirate osnovne brezžične in varnostne nastavitve mostu.

To lahko naredite na dva načina, ročno in s funkcijo Wi-Fi Protected Setup. Wi-Fi Protected Setup je funkcija, ki olajša nastavitev brezžičnega omrežja. Če omrežni usmerjevalnik podpira Wi-Fi Protected Setup in uporablja zaščito WPA ali WPA2, lahko most samodejno povežete s funkcijo Wi-Fi Protected Setup.

Configuration View (Pogled konfiguracije) Če želite brezžično omrežje konfigurirati ročno, izberite **Manual** (Ročno). Oglejte si **Basic Wireless Settings** (Osnovne brezžične nastavitve), **stran 8**. Če želite uporabiti Wi-Fi Protected Setup, izberite **Wi-Fi Protected Setup**. Oglejte si **Wi-Fi Protected Setup**, **stran 9**.

Basic Wireless Settings (Osnovne brezžične nastavitve)



Network Name (Ime omrežja) **(SSID)** SSID je ime omrežja, ki si ga delijo vse točke v brezžičnem omrežju. SSID mora biti za vse naprave v brezžičnem omrežju enak. Razlikuje med velikimi in malimi črkami in ne sme biti daljši od 32 znakov (uporabite lahko vse znake na tipkovnici). Preverite, ali se nastavitev ujema s tisto na brezžičnem usmerjevalniku ali dostopni točki. Za dodatno varnost privzet SSID (**linksys**) spremenite v edinstveno ime.

Wireless Security (Varnost brezžičnih omrežij)

Most podpira te možnosti zaščite brezžičnih omrežij: WPA – osebno, WPA2 – osebno in WEP. WPA (Wi-Fi Protected Access) in WPA2 sta varnejša načina zaščite kot WEP (Wired Equivalent Privacy). Za več informacij o varnosti brezžičnih omrežij si oglejte »Varnostni seznam za zaščito brezžičnega omrežja«, stran 4.

Security Mode (Varnostni način)

Izberite način zaščite brezžičnega omrežja. Če brezžičnega omrežja ne želite zaščititi, obdržite privzeto vrednost **Disabled** (Onemogočeno).

OPOMBA
Ne pozabite, da MORA vsaka naprava v brezžičnem omrežju uporabljati enak varnostni način in geslo ali ključ, drugače brezžične naprave med seboj ne bodo mogle komunicirati.

WPA – osebno

WPA je varnostni standard, močnejši od šifriranja WEP.



Encryption (Šifriranje) WPA podpira način šifriranja TKIP z dinamičnimi šifrirnimi ključi.

Passphrase (Geslo) Vnesite ključ, ki si ga delita most in brezžični usmerjevalnik ali dostopna točka. Imeti mora med 8 in 63 znaki.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

WPA2 – osebno

WPA2 je naprednejša in varnejša različica načina WPA.



Encryption (Šifriranje) WPA2 podpira dva načina šifriranja z dinamičnimi šifrirnimi ključi – TKIP in AES. Izberite način šifriranja, **AES** ali **TKIP ali AES**. Privzeta izbira je **AES**.

Passphrase (Geslo) Vnesite ključ, ki si ga delita most in brezžični usmerjevalnik ali dostopna točka. Imeti mora med 8 in 63 znaki.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

WEP

WEP je osnovni varnostni način, ki ni tako varen kot WPA ali WPA2.



Encryption (Šifriranje) Izberite raven šifriranja WEP, **40/64 bits (10 hex digits)** (40/64-bitno (10 heksadecimalnih mest)) ali **104/128 bits (26 hex digits)** (104/128-bitno (26 heksadecimalnih mest)). Privzeta nastavitev je **40/64 bits (10 hex digits)** (40/64-bitno (10 heksadecimalnih mest)).

Key 1 (Ključ 1) Vnesite ključ WEP omrežja.

Tx Key (Ključ za oddajanje) **Ključ 1** je ključ za oddajanje, ki ga uporablja most.

Authentication (Preverjanje pristnosti) Privzeta nastavitev je **Auto** (Samodejno), ki omogoča odprto sistemsko preverjanje ali preverjanje pristnosti skupnega ključa. Izberite **Open** (Odprto), če želite uporabljati odprto sistemsko preverjanje pristnosti; pošiljatelj in prejemnik za preverjanje pristnosti ne uporabljata ključa WEP. Izberite **Shared** (Skupno), če želite uporabljati preverjanje pristnosti skupnega ključa; pošiljatelj in prejemnik za preverjanje pristnosti uporabljata ključ WEP.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Wi-Fi Protected Setup

Na voljo sta dva načina. Uporabite tistega, ki je primeren za usmerjevalnik, ki ga uporabljate.





1. način

Ta način uporabite, če ima usmerjevalnik gumb Wi-Fi Protected Setup.

1. Kliknite ali pritisnite gumb **Wi-Fi Protected Setup** na usmerjevalniku.
2. V dveh minutah kliknite gumb **Wi-Fi Protected Setup** na zaslonu *Wi-Fi Protected Setup* mostu.
3. Po konfiguraciji mostu kliknite **Close** (Zapri).

Na zaslonu *Wi-Fi Protected Setup* so prikazane možnosti Link Status (Stanje povezave), Network Name (Ime omrežja) (SSID) in Security method (Varnostni način).

2. način

Ta način uporabite, če usmerjevalnik zahteva številko PIN mostu.

1. Na zaslonu *Wi-Fi Protected Setup* **usmerjevalnika** vnesite številko PIN, ki je na zaslonu *Wi-Fi Protected Setup* **mostu**. Nato kliknite **Register** (Registriraj) ali ustrezen gumb. (Prikazan je tudi na nalepki na spodnji strani mostu.)
2. Na zaslonu *Wi-Fi Protected Setup* **mostu** kliknite **OK** (V redu).
3. Po konfiguraciji mostu kliknite **Close** (Zapri).

Na zaslonu *Wi-Fi Protected Setup* so prikazane možnosti Link Status (Stanje povezave), Network Name (Ime omrežja) (SSID) in Security method (Varnostni način).

Wireless (Brezžična povezava) > Wireless Network Site Survey (Pregled mest brezžičnega omrežja)

Za začetek pregleda kliknite zavihek **Wireless Network Site Survey** (Pregled mest brezžičnega omrežja). Na zaslonu *Wireless Network Site Survey* (Pregled mest brezžičnega omrežja) so našteta brezžična omrežja, ki jih je zaznal most.



Wireless Network Site Survey (Pregled mest brezžičnega omrežja)

Number of Wireless Networks (Število brezžičnih omrežij) Prikazano je število brezžičnih omrežij, ki jih je zaznal most.

Select (Izberi) Če želite vzpostaviti povezavo z brezžičnim omrežjem, kliknite **Select** (Izberi) in nato še **Connect** (Vzpostavi povezavo).

Wireless Network Name (Ime brezžičnega omrežja) Prikazano je ime ali SSID brezžičnega omrežja.

GHz Prikazan je radijski frekvenčni pas brezžičnega omrežja.

Signal Prikazan je odstotek moči signala. 100 % je najmočnejši mogoč signal; 0 % je najšibkejši mogoč.

Security (Varnost) Če omrežje podpira Wi-Fi Protected Setup, je prikazana ikona Wi-Fi Protected Setup . Prikazan je varnostni način, ki ga uporablja omrežje.

Če želite posodobiti podatke na zaslonu, kliknite **Refresh** (Osveži).

Po izbiri omrežja kliknite **Connect** (Vzpostavi povezavo). Prikaže se nov zaslon. Sledite navodilom za varnostni način vašega omrežja.

WPA



Network Name (Ime omrežja) **(SSID)** Samodejno je prikazano ime izbranega omrežja.

Security Mode (Varnostni način) Samodejno je prikazan WPA – osebno.

Encryption (Šifriranje) WPA podpira način šifriranja TKIP z dinamičnimi šifrirnimi ključi.

Passphrase (Geslo) Vnesite ključ, ki si ga delita most in brezžični usmerjevalnik ali dostopna točka. Imeti mora med 8 in 63 znaki.

Če želite posodobiti podatke na zaslonu, kliknite **Refresh** (Osveži).

Po vnosu varnostnih nastavitev kliknite **Connect** (Vzpostavi povezavo).

WPA2



Network Name (Ime omrežja) **(SSID)** Samodejno je prikazano ime izbranega omrežja.

Security Mode (Varnostni način) Samodejno je prikazan WPA2 – osebno.

Encryption (Šifriranje) WPA2 podpira dva načina šifriranja z dinamičnimi šifrirnimi ključi – TKIP in AES. Izberite način šifriranja, **AES** ali **TKIP ali AES**.

Passphrase (Geslo) Vnesite ključ, ki si ga delita most in brezžični usmerjevalnik ali dostopna točka. Imeti mora med 8 in 63 znaki.

Če želite posodobiti podatke na zaslonu, kliknite **Refresh** (Osveži).

Po vnosu varnostnih nastavitev kliknite **Connect** (Vzpostavi povezavo).

WEP



Network Name (Ime omrežja) **(SSID)** Samodejno je prikazano ime izbranega omrežja.

Security Mode (Varnostni način) Samodejno je prikazan WEP.

Encryption (Šifriranje) Izberite raven šifriranja WEP **40/64 bits (10 hex digits)** (40/64-bitno (10 heksadecimalnih mest)) ali **104/128 bits (26 hex digits)** (104/128-bitno (26 heksadecimalnih mest)).

Key 1 (Ključ 1) Vnesite ključ WEP omrežja.

Tx Key (Ključ za oddajanje) **Ključ 1** je ključ za oddajanje, ki ga uporablja most.

Authentication (Preverjanje pristnosti) Privzeta nastavitev je **Auto** (Samodejno), ki omogoča odprto sistemsko preverjanje ali preverjanje pristnosti skupnega ključa. Izberite **Open** (Odprto), če želite uporabljati odprto sistemsko preverjanje pristnosti; pošiljatelj in prejemnik za preverjanje pristnosti ne uporabljata ključa WEP. Izberite **Shared** (Skupno), če želite uporabljati preverjanje pristnosti skupnega ključa; pošiljatelj in prejemnik za preverjanje pristnosti uporabljata ključ WEP.

Če želite posodobiti podatke na zaslonu, kliknite **Refresh** (Osveži).

Po vnosu varnostnih nastavitev kliknite **Connect** (Vzpostavi povezavo).

Wireless (Brezžična povezava) > WMM®

Konfigurirajte nastavitve brezžične večpredstavnosti (WMM). WMM določa prioriteto paketov glede na njihov način dostopa (vrsto prometa): Background (Ozadje), Best Effort (Najvztrajnejše), Video (Video) ali Voice (Glas). Te nastavitve naj prilagodi izkušen skrbnik, saj lahko napačne nastavitve znižajo učinkovitost delovanja brezžičnega omrežja.



OPOMBA
Nastavitve na zaslonu *WMM* so namenjene samo naprednim uporabnikom.

WMM

Access Mode (Način dostopa)

Štirim razpoložljivim načinom dostopa lahko dodelite različne nastavitve. Izberite način, ki ga želite konfigurirati: **Background** (Ozadje), **Best Effort** (Najvztrajnejše), **Video** (Video) ali **Voice** (Glas). Sledite navodilom za izbran način.

Background (Ozadje)

Use Aggregation (Uporabi združevanje) Ta možnost določa, ali naj plast MAC (Media Access Control) vzpostavi sejo ADDBA (Add Block Acknowledgement). Privzeta vrednost je **No** (Ne). Če želite možnost omogočiti, izberite **Yes** (Da).

Accept Aggregation (Sprejmi združevanje) Ta možnost določa, ali naj plast MAC sprejme zahtevo ADDBA. Privzeta vrednost je **Yes** (Da). Če želite možnost onemogočiti, izberite **No** (Ne).

Max. Number of Packets in Aggregation (Največje število paketov pri združevanju) Ta možnost določa največje število paketov (podokvirjev) pri združevanju. Dovoljen obseg je med **0** in **7**. Privzeta vrednost je **7**.

Max. Aggregation Size (Največja velikost združevanja) Ta možnost določa največjo velikost združka (v bajtih). Dovoljen obseg je med **0** in **16000**. Privzeta vrednost je **12000**.

Timeout Internal (Notranja časovna omejitev) Ta možnost določa časovno omejitev, po kateri naj se združek zapre s "stanjem zapiranja", preden ga zapre časovnik. Dovoljen obseg je med **0** in **100** ms. Privzeta vrednost je **3**.

Min. Size of Packet in Aggregation (Najmanjša velikost paketa pri združevanju) Ta možnost določa najmanjšo velikost (v bajtih) paketov za združevanje. Dovoljen obseg je med **0** in **1500**. Privzeta vrednost je **10**.

ADDBA Timeout (Časovna omejitev za ADDBA) Ta možnost določa trajanje, po katerem se nastavitev za ADDBA prekine, če med tem ni izmenjav po sporazumu ACK (Block Acknowledgement). Dovoljen obseg je med **0** in **65535** ms. Privzeta vrednost je **0**, kar onemogoči časovno omejitev.

Aggregation Window Size (Velikost okna združevanja) Ta možnost določa največje število oddanih paketov brez prejetja potrditev. Dovoljen obseg je med **0** in **64**. Privzeta vrednost je **64**.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Best Effort (Najvztrajnejše)

Use Aggregation (Uporabi združevanje) Ta možnost določa, ali naj plast MAC (Media Access Control) vzpostavi sejo ADDBA (Add Block Acknowledgement). Privzeta vrednost je **Yes** (Da). Če želite možnost onemogočiti, izberite **No** (Ne).

Accept Aggregation (Sprejmi združevanje) Ta možnost določa, ali naj plast MAC sprejme zahtevo ADDBA. Privzeta vrednost je **Yes** (Da). Če želite možnost onemogočiti, izberite **No** (Ne).

Max. Number of Packets in Aggregation (Največje število paketov pri združevanju) Ta možnost določa največje število paketov (podokvirjev) pri združevanju. Dovoljen obseg je med **0** in **10**. Privzeta vrednost je **10**.

Max. Aggregation Size (Največja velikost združevanja) Ta možnost določa največjo velikost združka (v bajtih). Dovoljen obseg je med **0** in **20000**. Privzeta vrednost je **16000**.

Timeout Internal (Notranja časovna omejitev) Ta možnost določa časovno omejitev, po kateri naj se združek zapre s "stanjem zapiranja", preden ga zapre časovnik. Dovoljen obseg je med **0** in **100** ms. Privzeta vrednost je **3**.

Min. Size of Packet in Aggregation (Najmanjša velikost paketa pri združevanju) Ta možnost določa najmanjšo velikost (v bajtih) paketov za združevanje. Dovoljen obseg je med **0** in **1500**. Privzeta vrednost je **10**.

ADDBA Timeout (Časovna omejitev za ADDBA) Ta možnost določa trajanje, po katerem se nastavitev za ADDBA prekine, če med tem ni izmenjav po sporazumu ACK (Block Acknowledgement). Dovoljen obseg je med **0** in **65535** ms. Privzeta vrednost je **0**, kar onemogoči časovno omejitev.

Aggregation Window Size (Velikost okna združevanja) Ta možnost določa največje število oddanih paketov brez prejetja potrditev. Dovoljen obseg je med **0** in **64**. Privzeta vrednost je **64**.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Video (Video)

Use Aggregation (Uporabi združevanje) Ta možnost določa, ali naj plast MAC (Media Access Control) vzpostavi sejo ADDBA (Add Block Acknowledgement). Privzeta vrednost je **Yes** (Da). Če želite možnost onemogočiti, izberite **No** (Ne).

Accept Aggregation (Sprejmi združevanje) Ta možnost določa, ali naj plast MAC sprejme zahtevo ADDBA. Privzeta vrednost je **Yes** (Da). Če želite možnost onemogočiti, izberite **No** (Ne).

Max. Number of Packets in Aggregation (Največje število paketov pri združevanju) Ta možnost določa največje število paketov (podokvirjev) pri združevanju. Dovoljen obseg je med **0** in **7**. Privzeta vrednost je **7**.

Max. Aggregation Size (Največja velikost združevanja) Ta možnost določa največjo velikost združka (v bajtih). Dovoljen obseg je med **0** in **16000**. Privzeta vrednost je **12000**.

Timeout Internal (Notranja časovna omejitev) Ta možnost določa časovno omejitev, po kateri naj se združek zapre s "stanjem zapiranja", preden ga zapre časovnik. Dovoljen obseg je med **0** in **100** ms. Privzeta vrednost je **3**.

Min. Size of Packet in Aggregation (Najmanjša velikost paketa pri združevanju) Ta možnost določa najmanjšo velikost (v bajtih) paketov za združevanje. Dovoljen obseg je med **0** in **1500**. Privzeta vrednost je **10**.

ADDBA Timeout (Časovna omejitev za ADDBA) Ta možnost določa trajanje, po katerem se nastavitev za ADDBA prekine, če med tem ni izmenjav po sporazumu ACK (Block Acknowledgement). Dovoljen obseg je med **0** in **65535** ms. Privzeta vrednost je **0**, kar onemogoči časovno omejitev.

Aggregation Window Size (Velikost okna združevanja) Ta možnost določa največje število oddanih paketov brez prejetja potrditev. Dovoljen obseg je med **0** in **64**. Privzeta vrednost je **64**.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Voice (Glas)

Use Aggregation (Uporabi združevanje) Ta možnost določa, ali naj plast MAC (Media Access Control) vzpostavi sejo ADDBA (Add Block Acknowledgement). Privzeta vrednost je **Yes** (Da). Če želite možnost onemogočiti, izberite **No** (Ne).

Accept Aggregation (Sprejmi združevanje) Ta možnost določa, ali naj plast MAC sprejme zahtevo ADDBA. Privzeta vrednost je **Yes** (Da). Če želite možnost onemogočiti, izberite **No** (Ne).

Max. Number of Packets in Aggregation (Največje število paketov pri združevanju) Ta možnost določa največje število paketov (podokvirjev) pri združevanju. Dovoljen obseg je med **0** in **2**. Privzeta vrednost je **2**.

Max. Aggregation Size (Največja velikost združevanja) Ta možnost določa največjo velikost združka (v bajtih). Dovoljen obseg je med **0** in **16000**. Privzeta vrednost je **10000**.

Timeout Internal (Notranja časovna omejitev) Ta možnost določa časovno omejitev, po kateri naj se združek zapre s "stanjem zapiranja", preden ga zapre časovnik. Dovoljen obseg je med **0** in **100** ms. Privzeta vrednost je **10**.

Min. Size of Packet in Aggregation (Najmanjša velikost paketa pri združevanju) Ta možnost določa najmanjšo velikost (v bajtih) paketov za združevanje. Dovoljen obseg je med **0** in **1500**. Privzeta vrednost je **10**.

ADDBA Timeout (Časovna omejitev za ADDBA) Ta možnost določa trajanje, po katerem se nastavitev za ADDBA prekine, če med tem ni izmenjav po sporazumu ACK (Block Acknowledgement). Dovoljen obseg je med **0** in **65535** ms. Privzeta vrednost je **0**, kar onemogoči časovno omejitev.

Aggregation Window Size (Velikost okna združevanja) Ta možnost določa največje število oddanih paketov brez prejetja potrditev. Dovoljen obseg je med **0** in **64**. Privzeta vrednost je **64**.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Wireless (Brezžična povezava) > Advanced Wireless Settings (Dodatne brezžične nastavitve)

Konfigurirajte dodatne brezžične funkcije mostu. Te nastavitve naj prilagodi izkušen skrbnik, saj lahko napačne nastavitve znižajo učinkovitost delovanja brezžičnega omrežja.



OPOMBA
Nastavitve na zaslonu *Advanced Wireless Settings* (Dodatne brezžične nastavitve) so namenjene samo naprednim uporabnikom.

Advanced Wireless (Dodatne nastavitve brezžične povezave)

Use LDPC (Uporabi LDPC) Koda za preverjanje parnosti z nizko gostoto (LDPC) omogoči ali onemogoči odpravljanje napak za zmanjšanje možnosti izgube podatkov v kanalih z veliko šuma. Algoritem za prilagajanje hitrosti prenosa samodejno onemogoči kodiranje LDPC pri delu z visokimi hitrostmi fizične plasti (višje od 162). Če želite uporabljati dodatno shemo LDCP za odpravljanje napak, obdržite privzeto vrednost **Yes** (Da). V nasprotnem primeru izberite **No** (Ne).

ERP Protection Type (Vrsta zaščite ERP) Ta možnost konfigurira zaščito paketov OFDM kljub prisotnosti naprav 802.11b v brezžičnem omrežju. S pošiljanjem paketov RTS/CTS ali CTS2Self s hitrostmi prenosa 802.11b most pove brezžičnemu omrežju, da bo prenašal pakete OFDM, in jih v brezžičnem omrežju zaščiti. Paketi RTS/CTS in CTS2Self ustvarijo dodaten promet, kar lahko pomeni nižjo prepustnost.

Možnost RTS/CTS zagotavlja v primerjavi s CTS2Self boljšo pokritost, vendar zniža prepustnost, ker vključuje potrdila iz ciljne naprave. Če želite uporabiti možnost RTS/CTS, obdržite privzeto vrednost **RTS/CTS**. Možnost None (Brez) lahko povzroči spore med paketi OFDM in CCK. Če jo želite vseeno uporabiti, izberite **None** (Brez). Če želite uporabiti možnost CTS2Self, izberite **CTS2Self**.

11n Protection Type (Vrsta zaščite 11n) Ta možnost konfigurira zaščito pred napravami z nizko prepustnostjo (HT) v brezžičnem omrežju. Če brezžični usmerjevalnik (ali dostopna točka) zazna povezavo s starejšo napravo z nizko prepustnostjo, bo vsem napravam z nizko prepustnostjo sporočil, da morajo pred vsakim oddajanjem podatkov uporabiti mehanizem RTS/CTS ali CTS2Self. Funkcija podpira tudi običajne zaščite 802.11n, vključno z MIMO.

Možnost RTS/CTS zagotavlja v primerjavi s CTS2Self boljšo pokritost, vendar zniža prepustnost, ker vključuje potrdila iz ciljne naprave. Če želite uporabiti možnost RTS/CTS, obdržite privzeto vrednost **RTS/CTS**. Možnost None (Brez) lahko povzroči spore med paketi HT in starejšimi paketi. Če jo želite vseeno uporabiti, izberite **None** (Brez). Če želite uporabiti možnost CTS2Self, izberite **CTS2Self**.

Percentage of maximal transmit power (Odstotek največje oddajne moči) Ta možnost določa odstotek največje oddajne moči glede na pravne omejitve za domeno. Če pravna omejitev za domeno na primer dovoljuje oddajno moč do 20 dB, potem bo vrednost 50 % dovoljevala največjo oddajno moč 10 dB. Izberite odstotek, ki ga želite uporabiti: **12 %**, **25 %**, **50 %** ali **100 %**. Privzeta vrednost je **100 %**.

QoS Classification Type (Vrsta razvrščanja QoS) Ta možnost določa prioritete za preslikovanje 802.1D ali 802.1Q iz polja IP DSCP/TOS v WMM (ozadje, najvztrajnejše, video in glas). Obdržite privzeto vrednost **802.1D** ali izberite **802.1Q**, ki jo uporabljajo nekateri tokovi za televizijo IP.

Re-establish Ethernet connection when initiating wireless connection (Pri vzpostavljanju brezžične povezave znova vzpostavi ethernetno povezavo) Za sprožitev odkrivanja strežnika DHCP naprave, ki je za mostom, bo most pri vsakem vzpostavljanju brezžične povezave ponastavil ethernetno povezavo med mostom in napravo. Če želite onemogočiti to obnašanje, izberite **No** (Ne). V nasprotnem primeru izberite privzeto vrednost **Yes** (Da).

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Administration (Skrbništvo) > Management (Upravljanje)

Na tem zaslonu lahko upravljate določene funkcije mostu: dostop do pripomočka v brskalniku, varnostno kopiranje konfiguracijske datoteke in ponovni zagon.



Management (Upravljanje)

Bridge Access (Dostop do mostu)

Dostop do pripomočka v brskalniku zaščitite z geslom.

Bridge Password (Geslo za most) Vnesite novo geslo za most.

Re-enter to confirm (Ponovni vnos za potrditev) Za potrditev geslo vnesite še enkrat.

Idle Timeout (Časovna omejitev nedejavnosti) Prijava se po navedenem obdobju nedejavnosti prekine. Dovoljen obseg je med **60** in **3600** sekund. Privzeta vrednost je **600**.

Web Access (Dostop do spleta)

Access via Wireless (Dostop prek brezžične povezave) Če most uporabljate v javni domeni, kjer gostom omogočate brezžičen dostop, lahko onemogočite brezžičen dostop do pripomočka mostu v brskalniku. Če to možnost onemogočite, boste lahko do pripomočka v brskalniku dostopali le prek žične povezave. Če želite dovoliti brezžičen dostop do pripomočka mostu v brskalniku, obdržite privzeto vrednost **Enabled** (Omogočeno), če pa želite blokirati brezžičen dostop do pripomočka, izberite **Disabled** (Onemogočeno).

Backup and Restore (Varnostno kopiranje in obnovitev)

Backup (Varnostno kopiranje) Če želite varnostno kopirati konfiguracijsko datoteko mostu, kliknite **Backup Configurations** (Varnostno kopiraj konfiguracije). Nato sledite navodilom na zaslonu.

Restore (Obnovitev) Kliknite **Browse** (Prebrskaj) in izberite konfiguracijsko datoteko. Kliknite **Restore Configurations** (Obnovi konfiguracije).

System Reboot (Ponovni zagon sistema)

Reboot (Ponovni zagon) Če želite ponovno zagnati most, kliknite Start to Reboot (Začni ponovni zagon) **Začni ponovni zagon**.

Kliknite **Save Settings** (Shrani nastavitve), da spremembe uporabite, ali **Cancel Changes** (Prekliči spremembe), da jih prekličete.

Administration (Skrbništvo) > Factory Defaults (Tovarniško privzete vrednosti)

Na tem zaslonu lahko konfiguracijo mostu ponastavite na tovarniško privzete vrednosti.

Factory Defaults (Tovarniško privzete vrednosti)

Restore All Settings (Obnovi vse nastavitve) Če želite nastavitve mostu ponastaviti na tovarniško privzete vrednosti, kliknite **Restore All Settings** (Obnovi vse nastavitve). Vse shranjene nastavitve bodo ob obnovitvi privzetih nastavitev izgubljene.



Administration (Skrbništvo) > Upgrade Firmware (Nadgradnja vgrajene programske opreme)

Na tem zaslonu lahko nadgradite vgrajeno programsko opremo mostu. Vgrajeno programsko opremo nadgradite le, če imate z mostom težave ali pa ima nova programska oprema funkcijo, ki jo želite uporabljati.



Pred nadgradnjo vgrajene programske opreme s spletnega mesta Linksys, **www.Linksys.com/support**, prenesite datoteko za nadgradnjo vgrajene programske opreme mostu.

Upgrade Firmware (Nadgradnja vgrajene programske opreme)

Please select a file to upgrade the firmware (Izberite datoteko, s katero želite nadgraditi vgrajeno programsko opremo) Kliknite **Browse** (Prebrskaj) in izberite datoteko za nadgradnjo vgrajene programske opreme. Nato kliknite **Start to Upgrade** (Začni nadgradnjo) in sledite navodilom na zaslonu.

Status (Stanje) > Bridge (Most)

Prikazane so informacije o trenutnem stanju mostu.



Bridge Information (Informacije o mostu)

Firmware Version (Različica vgrajene programske opreme) Prikazana je trenutna programska oprema, vgrajena v most.

Local Network (Lokalno omrežje)

Local MAC Address (Lokalni naslov MAC) Prikazan je naslov MAC mostu, kot je viden v lokalnem ethernetnem omrežju.

IP Address (Naslov IP) Prikazan je naslov IP mostu, kot je viden v lokalnem ethernetnem omrežju.

Subnet Mask (Maska podomrežja) Prikazana je maska podomrežja, ki je konfigurirana za lokalno omrežje.

Status (Stanje) > Wireless (Brezžična povezava)

Prikazane so informacije o brezžičnem omrežju.



Wireless (Brezžična povezava)

Link Status (Stanje povezave) Prikazano je stanje povezave z brezžičnim omrežjem.

MAC Address (Naslov MAC) Prikazan je naslov MAC mostu, kot je viden v lokalnem brezžičnem omrežju.

Network Name (Ime omrežja) **(SSID)** Prikazano je ime ali SSID brezžičnega omrežja.

BSSID Prikazan je naslov MAC povezanega brezžičnega usmerjevalnika (ali dostopne točke).

Radio Band (Radijski frekvenčni pas) Prikazan je radijski frekvenčni pas brezžičnega omrežja.

Channel Width (Širina kanala) Prikazana je širina kanala (v MHz), ki ga uporablja brezžično omrežje.

Wide Channel (Širok kanal) Odvisno od nastavitve kanala za omrežni usmerjevalnik je prikazana možnost Wide Channel (Širok kanal). Če ste za možnost usmerjevalnika Radio Band (Radijski frekvenčni pas) ali Channel Width (Širina kanala) izbrali Wide - 40MHz Channel (Širok kanal – 40 MHz), bo to primarni kanal za protokol Wireless-N.

Standard Channel (Standardni kanal) Prikazana je nastavitev Standard Channel (Standardni kanal). Če ste za možnost usmerjevalnika Radio Band (Radijski frekvenčni pas) ali Channel Width (Širina kanala) izbrali Wide - 40MHz Channel (Širok kanal – 40 MHz), bo standardni kanal sekundarni kanal za protokol Wireless-N.

Bit Rate (Hitrost prenosa) Prikazana je hitrost prenosa podatkov.

Signal Prikazan je odstotek moči signala. 100 % je najmočnejši mogoč signal; 0 % je najšibkejši mogoč.

Security (Varnost) Prikazan je način zaščite brezžičnega omrežja.

Odpravljanje napak

WES610N/WET610N

Računalnik ali druge žične ethernetne naprave ne morejo komunicirati z brezžičnim usmerjevalnikom.

1. Odprite pripomoček mostu v brskalniku.
2. Na zaslonu *Basic Wireless Settings* (Osnovne brezžične nastavitve) preverite, ali se ime omrežja (SSID) ujema z imenom brezžičnega omrežja.
3. Preverite, ali se varnostne nastavitve (WPA, WPA2 ali WEP) ujemajo z varnostnimi nastavitvami brezžičnega omrežja.

Naslov IP mostu morate spremeniti.

Če je most povezan z omrežjem, ki ima strežnik DHCP (običajno usmerjevalnik omrežja), bo most naslov IP pridobil pri strežniku DHCP. Če strežnika DHCP ni, bo most uporabil privzet statičen naslov IP **169.254.1.250**.

Če želite, da most vedno uporablja statičen naslov IP, sledite tem navodilom:

1. Odprite pripomoček mostu v brskalniku.
2. Kliknite zavihek **Network Setup** (Nastavitev omrežja).
3. Na spustnem meniju *Network Connection Type* (Vrsta omrežne povezave) izberite **Static IP** (Statičen IP).
4. Izpolnite polja *Static IP Address* (Statičen naslov IP), *Subnet Mask* (Maska podomrežja) in *Default Gateway* (Privzet prehod).
5. Kliknite **Save Settings** (Shrani nastavitve).

Računalnik, ki lahko uporablja most, ali druga žična ethernetna naprava ne komunicira z drugo napravo z brezžično povezavo (na primer računalnik ali tiskalnik).

Preverite:

- Preverite, ali je naprava z brezžično povezavo v istem brezžičnem omrežju kot računalnik ali druga žična ethernetna naprava povezana z mostom.
- Preverite, ali vse naprave v brezžičnem omrežju uporabljajo enako ime omrežja (SSID).
- Preverite, ali so vse naprave v omrežju z enakim naslovom IP in uporabljajo združljive naslove IP.

Pripomoček v brskalniku ne sprejme gesla.

Preverite:

- Geslo razlikuje med malimi in velikimi črkami. Preverite, ali pri vnašanju gesla pravilno uporabljate male in velike črke.
- Če pozabite geslo, lahko most ponastavite na tovarniško privzete vrednosti.

 Pritisnite in približno pet sekund držite gumb za **ponastavitev** na mostu; geslo se bo ponastavilo na tovarniško privzeto vrednost **admin**. Vse druge nastavitve mostu se bodo prav tako ponastavile na tovarniško privzete vrednosti. (Za dostop do pripomočka v brskalniku v polje *Pasword* (Geslo) vnesite **admin**.)

Če nastavitve spremenite v pripomočku v brskalniku, nove nastavitve ne bodo prikazane na zaslonu.

V brskalniku kliknite **Osveži**. Če se nove nastavitve še vedno ne prikažejo, sledite tem navodilom:

1. Napajalnik odklopite od mostu.
2. Počakajte pet sekund, nato pa napajalnik priklopite nazaj na most.
3. V brskalniku kliknite **Osveži**.

SPLET
Če odgovorov na vprašanja tukaj ne morete najti, si oglejte spletno mesto Linksys na naslovu **Linksys.com/support**.

Specifikacije

WES610N

Model	WES610N
Standardi	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Indikatorji	vklop/izklop, ethernet, Wi-Fi Protected Setup™, brezžična povezava, posamezna ethernetna povezava in aktivnost
Vrata	ethernet (4), napajanje
Gumba	ponastavitev, Wi-Fi Protected Setup
Vrsta kablov	CAT5e
Antene	3 (notranje)
Vrsta priključkov anten	ni na voljo
Snemljivo (da/ne)	ne
Modulacije	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Radiofrekvenčna moč (EIRP) v dBm	802.11a: 15 dBm (običajno) pri 54 Mb/s 802.11b: 19 dBm (običajno) pri 11 Mb/s 802.11g: 16 dBm (običajno) pri 54 Mb/s 802.11n (2,4 GHz): 18 dBm (običajno) pri MCS15 802.11n (5 GHz): 16 dBm (običajno) pri MCS15
Občutljivost prejemanja	802.11a: -72 dBm (običajno) pri 54 Mb/s 802.11b: -85 dBm (običajno) pri 11 Mb/s 802.11g: -73 dBm (običajno) pri 54 Mb/s 802.11n (20 MHz): -75 dBm (običajno) pri MCS15 802.11n (40 MHz): -69 dBm (običajno) pri MCS15
Ojačanje antene v dBi	1
Zaščita brezžičnega omrežja	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Vrsta varnostnega ključa	do 128-bitno šifriranje

Okoljski podatki

Dimenzije	177 x 128 x 68 mm (6,97 x 5,04 x 2,68 palca)
Teža	295 g (0,65 lb)
Potrdila	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Napajanje	12 V, 1 A
Temperatura za delovanje	od 0 do 40 °C (od 32 do 104 °F)
Temperatura za shranjevanje	od -20 do 60 °C (od -4 do 140 °F)
Vlažnost za delovanje	od 10 do 85 %, brez kondenzacije
Vlažnost za shranjevanje	od 5 do 90 %, brez kondenzacije

Specifikacije se lahko spremenijo brez predhodnega obvestila.

WET610N

Model	WET610N
Standardi	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Indikatorji	vklop/izklop, ethernet, Wi-Fi Protected Setup™, brezžična povezava
Vrata	ethernet, napajanje
Gumba	ponastavitev, Wi-Fi Protected Setup
Vrsta kablov	CAT5e
Antene	3 (notranje)
Vrsta priključkov anten	ni na voljo
Snemljivo (da/ne)	ne
Modulacije	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Radiofrekvenčna moč (EIRP) v dBm	802.11a: 15 dBm (običajno) pri 54 Mb/s 802.11b: 18 dBm (običajno) pri 11 Mb/s 802.11g: 16 dBm (običajno) pri 54 Mb/s 802.11n: 12 dBm (običajno) pri 130 Mb/s (HT20), 270 Mb/s (HT40)
Občutljivost prejemanja	802.11a: -72 dBm (običajno) pri 54 Mb/s 802.11b: -85 dBm (običajno) pri 11 Mb/s 802.11g: -73 dBm (običajno) pri 54 Mb/s 802.11n: -70 dBm (običajno) pri MCS15/2,4 GHz, -69 dBm (običajno) pri MCS15/5,0 GHz
Ojačanje antene v dBi	1
Zaščita brezžičnega omrežja	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Vrsta varnostnega ključa	do 128-bitno šifriranje

Okoljski podatki

Dimenzije	145 x 106 x 52 mm (5,71 x 4,17 x 2,05 palca)
Teža	159 g (5,61 oz)
Potrdila	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Napajanje	12 V, 1 A
Temperatura za delovanje	od 0 do 40 °C (od 32 do 104 °F)
Temperatura za shranjevanje	od -20 do 60 °C (od -4 do 140 °F)
Vlažnost za delovanje	od 10 do 85 %, brez kondenzacije
Vlažnost za shranjevanje	od 5 do 90 %, brez kondenzacije

Specifikacije se lahko spremenijo brez predhodnega obvestila.

Linksys.com/support

Cisco, logotip Cisco in Linksys so blagovne znamke ali registrirane blagovne znamke družbe Cisco in/ali njenih hčerinskih družb v ZDA in določenih drugih državah.
Seznam blagovnih znamk družbe Cisco najdete na naslovu www.cisco.com/go/trademarks. Vse druge blagovne znamke, omenjene v tem dokumentu, so last njihovih lastnikov.

© 2011 Cisco in/ali njegove hčerinske družbe. Vse pravice pridržane.

3425-01249



คู่มือผู้ใช้

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

เนื้อหา

ภาพรวมผลิตภัณฑ์

LED panel (แผงไฟ LED) 2
Ports panel (แผงของพอร์ต) 3

Wireless Security Checklist (รายการตรวจสอบการรักษาความปลอดภัยไร้สาย)

เปลี่ยนชื่อดีฟอลต์ของเครือข่ายไร้สาย หรือ SSID 4
เปลี่ยนรหัสผ่านที่เป็นดีฟอลต์ 4
เปิดใช้งานการกรองแอดเดรส MAC 4
เปิดใช้การเข้ารหัส 4

คำแนะนำการรักษาความปลอดภัยเครือข่ายทั่วไป 4
เคล็ดลับในการรักษาความปลอดภัยเพิ่มเติม 5

การตั้งค่าขั้นสูง

วิธีการเข้าใช้ยูทิลิตีบนเบราว์เซอร์ 6
Setup (การตั้งค่า) > Basic Setup (การตั้งค่าพื้นฐาน) 7
Language (ภาษา) 7
การตั้งค่าเครือข่าย 7
Wireless (ระบบไร้สาย) > Basic Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน) 7
Basic Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน) 8
Wireless Security (การรักษาความปลอดภัยแบบไร้สาย) 8
Wi-Fi Protected Setup (การตั้งค่าแบบป้องกัน Wi-Fi) 9
Wireless (ระบบไร้สาย) > Wireless Network Site Survey (แบบสำรวจไซต์เครือข่ายไร้สาย) 10
Wireless Network Site Survey (แบบสำรวจไซต์เครือข่ายไร้สาย) 10
Wireless (ระบบไร้สาย) > WMM® 11
WMM 12
Wireless (ระบบไร้สาย) > Advanced Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นสูง) 13
Advanced Wireless (เครือข่ายไร้สายขั้นสูง) 13
Administration (การดูแลระบบ) > Management (การจัดการ) 14
Management (การจัดการ) 14
Administration (การดูแลระบบ) > Factory Defaults (ค่าดีฟอลต์จากโรงงาน) 15
Factory Defaults (ค่าดีฟอลต์จากโรงงาน) 15
Administration (การดูแลระบบ) > Upgrade Firmware (อัปเกรดเฟิร์มแวร์) 15
Upgrade Firmware (อัปเกรดเฟิร์มแวร์) 15
Status (สถานะ) > Bridge (บริดจ์) 15
Bridge Information (ข้อมูลของบริดจ์) 16
Local Network (เครือข่ายภายใน) 16
Status (สถานะ) > Wireless (ระบบไร้สาย) 16
Wireless (ระบบไร้สาย) 16

การแก้ไขปัญหา

WES610N/WET610N 17

คุณสมบัติเฉพาะ

WES610N 18
WET610N 19

ภาพรวมผลิตภัณฑ์

ขอขอบคุณที่เลือกใช้ Linksys Dual-Band N Entertainment Bridge บริดจ์สามารถเชื่อมต่อกับอุปกรณ์เชื่อมต่อ Ethernet ผ่านสายใดๆ กับเครือข่ายไร้สายของคุณ บริดจ์รองรับ Wireless-N พร้อมกันได้สองความถี่ ดังนั้นจึงสามารถใช้ได้กับเราเตอร์หรือจุดเชื่อมต่อ Wireless-N, -G, -A หรือ -B ใดๆ สำหรับการติดตั้งครั้งแรก โปรดทำตามขั้นตอนในที่ใส่ซีดี สำหรับการตั้งค่าขั้นสูง ให้ใช้บูทิลิตีบนเบราว์เซอร์ที่ใช้ง่าย

LED panel (แผงไฟ LED)



WES610N WET610N

ระบบไร้สาย (สีน้ำเงิน) ไฟ LED ระบบไร้สายจะสว่างขึ้นเมื่อมีการเชื่อมต่อไร้สาย ไฟ LED จะกะพริบเมื่อบริดจ์ส่งหรือรับข้อมูลผ่านเครือข่ายไร้สาย

Wi-Fi Protected Setup Button (ปุ่มการตั้งค่าแบบป้องกัน Wi-Fi) หากเราเตอร์เครือข่ายของคุณสนับสนุน Wi-Fi Protected Setup และใช้การรักษาความปลอดภัย WPA หรือ WPA2 คุณจะสามารถใช้ Wi-Fi Protected Setup เชื่อมต่อบริดจ์ได้โดยอัตโนมัติ ในการใช้ Wi-Fi Protected Setup โปรดดูที่ "Wireless (ระบบไร้สาย) > Basic Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน)" ในหน้า 7

Wi-Fi Protected Setup LED (ไฟการตั้งค่าแบบป้องกัน Wi-Fi) (สีน้ำเงิน/สีเหลืองอำพัน) ไฟ LED จะกะพริบเป็นสีน้ำเงินเป็นเวลา 2 นาที ระหว่างขั้นตอน Wi-Fi Protected Setup ไฟจะสว่างเป็นสีน้ำเงิน เมื่อการรักษาความปลอดภัยไร้สายถูกเปิดการใช้งาน ถ้าเกิดความผิดพลาดระหว่างขั้นตอน Wi-Fi Protected Setup ไฟ LED สีเหลืองอำพันจะสว่างขึ้น ตรวจสอบให้แน่ใจว่าเราเตอร์เครือข่ายสนับสนุน Wi-Fi Protected Setup รอจนกว่าไฟ LED จะดับลง แล้วลองอีกครั้ง

Ethernet (สีน้ำเงิน) ไฟ LED ของ Ethernet จะสว่างขึ้นเมื่อมีการเชื่อมต่อไร้สาย ไฟ LED จะกะพริบเมื่อบริดจ์ส่งหรือรับข้อมูลผ่านพอร์ต Ethernet

เปิด/ปิด (สีน้ำเงิน) ไฟ LED เปิด/ปิดจะสว่างขึ้นเมื่อบริดจ์เปิดอยู่

Ports panel (แผงของพอร์ต)



WES610N WET610N

Ethernet The Ethernet เชื่อมต่อบริดจ์เข้ากับคอมพิวเตอร์หรืออุปกรณ์เครือข่าย Ethernet อื่นๆ WES610N มี 4 พอร์ต และ WET610N มีพอร์ตเดียว

Reset (รีเซ็ต) การรีเซ็ตบริดจ์กลับเป็นค่าดีฟอลต์จากโรงงานมีอยู่ 2 วิธี กดปุ่ม Reset ค้างไว้ประมาณ 5 วินาที หรือเรียกคืนค่าดีฟอลต์จาก Administration (การดูแลระบบ) > Factory Defaults (ค่าดีฟอลต์จากโรงงาน) ในยูทิลิตีบนเบราว์เซอร์ของบริดจ์ WES610N มีปุ่ม reset อยู่ด้านล่าง และ WET610N มีปุ่ม reset อยู่ที่ด้านหลังแผงของอร์ต

Power พอร์ต Power (สายไฟ) ใช้สำหรับเชื่อมต่อบริดจ์เข้ากับอะแดปเตอร์

Wireless Security Checklist (รายการตรวจสอบการรักษาความปลอดภัยไร้สาย)

เครือข่ายไร้สายนั้นติดตั้งได้ง่าย ดังนั้นบ้านที่มีการเข้าถึงอินเทอร์เน็ตความเร็วสูงจึงนำมาใช้ได้อย่างรวดเร็ว เนื่องจากเครือข่ายไร้สายทำงานโดยการส่งข้อมูลผ่านคลื่นวิทยุ จึงมีความเสี่ยงต่อการบุกรุกมากกว่าเครือข่ายที่ใช้สายแบบเก่า เช่นเดียวกับสัญญาณจากโทรศัพท์ไร้สายหรือมือถือของคุณ สัญญาณจากเครือข่ายไร้สายของคุณสามารถถูกดักจับได้ เนื่องจากคุณไม่สามารถป้องกันผู้อื่นจากการเชื่อมต่อเครือข่ายไร้สายของคุณด้วยตัวคุณเองได้ คุณจึงต้องทำตามขั้นตอนเพิ่มเติมนี้เพื่อรักษาความปลอดภัยเครือข่ายของคุณ

เปลี่ยนชื่อดีฟอลต์ของเครือข่ายไร้สาย หรือ SSID

อุปกรณ์ไร้สายมีชื่อดีฟอลต์ของเครือข่ายไร้สาย หรือ Service Set Identifier (SSID) ที่ตั้งมาจากโรงงาน นี่เป็นชื่อเครือข่ายไร้สายของคุณ และมีความยาวได้ถึง 32 อักขระ ผลิตภัณฑ์ไร้สายของ Linksys ใช้ **linksys** เป็นชื่อดีฟอลต์ของเครือข่ายไร้สาย คุณควรเปลี่ยนชื่อเครือข่ายไร้สายเป็นชื่อที่ไม่ซ้ำ เพื่อแยกเครือข่ายไร้สายของคุณออกจากเครือข่ายไร้สายอื่นๆ ที่อาจมีอยู่รอบๆ แต่ต้องไม่ใช่ข้อมูลส่วนตัว (เช่น หมายเลขประกันสังคมของคุณ) เพราะผู้อื่นจะเห็นข้อมูลนี้ได้เมื่อเรียกดูเครือข่ายไร้สาย

เปลี่ยนรหัสผ่านที่เป็นดีฟอลต์

สำหรับผลิตภัณฑ์ไร้สาย เช่น จุดเชื่อมต่อ หรือ เราเตอร์ คุณจะถูกถามรหัสผ่านเมื่อคุณต้องการเปลี่ยนการตั้งค่า อุปกรณ์เหล่านี้มีรหัสผ่านดีฟอลต์ที่ถูกตั้งมาจากโรงงาน รหัสผ่านที่เป็นค่าดีฟอลต์ของ Linksys คือ **admin** แฮกเกอร์รู้รหัสที่เป็นดีฟอลต์นี้ และอาจพยายามที่จะใช้เพื่อเข้าใช้อุปกรณ์เครือข่ายของคุณและเปลี่ยนการตั้งค่าเครือข่ายของคุณ เพื่อขัดขวางความเปลี่ยนแปลงไม่ได้รับอนุญาต ให้ตั้งรหัสผ่านเองเพื่อให้เดายากขึ้น

เปิดใช้งานการกรองแอดเดรส MAC

เราเตอร์ของ Linksys ให้คุณสามารถเปิดใช้งานการกรองแอดเดรส Media Access Control (MAC) แอดเดรส MAC เป็นชุดของตัวเลขและอักษรเฉพาะที่ถูกกำหนดให้กับอุปกรณ์เครือข่ายทุกชิ้น ด้วยการเปิดใช้งานการกรองแอดเดรส MAC จะให้การเข้าใช้เครือข่ายไร้สายกับอุปกรณ์ไร้สายที่มีแอดเดรส MAC ที่ระบุเท่านั้น ตัวอย่างเช่น คุณสามารถระบุแอดเดรส MAC ของคอมพิวเตอร์แต่ละเครื่องในบ้านของคุณ จึงมีเพียงคอมพิวเตอร์เหล่านั้นเท่านั้นที่สามารถเข้าใช้เครือข่ายไร้สายของคุณได้

เปิดใช้การเข้ารหัส

การเข้ารหัสป้องกันการส่งข้อมูลผ่านเครือข่ายไร้สาย Wi-Fi Protected Access (WPA/WPA2) และ Wired Equivalent Privacy (WEP) ให้ระดับการรักษาความปลอดภัยที่ต่างกันสำหรับการสื่อสารไร้สาย

เครือข่ายที่เข้ารหัสด้วย WPA/WPA2 มีความปลอดภัยมากกว่าเครือข่ายไร้สายที่เข้ารหัสด้วย WEP เนื่องจาก WPA/WPA2 ใช้การเข้ารหัสคีย์แบบไดนามิกเพื่อป้องกันข้อมูลในขณะที่ส่งผ่านไปตามคลื่นอากาศ คุณควรเปิดใช้การเข้ารหัสขั้นสูงสุดที่อุปกรณ์เครือข่ายของคุณสนับสนุน

WEP เป็นมาตรฐานการเข้ารหัสแบบเก่า และอาจเป็นตัวเลือกเดียวที่มีอยู่ในอุปกรณ์รุ่นเก่าที่ไม่สนับสนุน WPA

คำแนะนำการรักษาความปลอดภัยเครือข่ายทั่วไป

การรักษาความปลอดภัยเครือข่ายไร้สายจะไม่เกิดประโยชน์ หากเครือข่ายภายในไม่มีการรักษาความปลอดภัย

- รหัสผ่านป้องกันคอมพิวเตอร์ทุกเครื่องในเครือข่าย และรหัสผ่านที่ต่างกันป้องกันไฟล์สำคัญ
- เปลี่ยนรหัสผ่านอยู่เสมอ
- ติดตั้งซอฟต์แวร์ป้องกันไวรัส และซอฟต์แวร์ Personal Firewall
- ปิดการใช้ไฟล์ร่วมกัน (peer-to-peer) การใช้งานบางอย่างอาจเปิดการใช้ไฟล์ร่วมกันโดยที่คุณไม่รู้หรือยินยอม

เคล็ดลับในการรักษาความปลอดภัยเพิ่มเติม

- ระวังให้เราเตอร์ไร้สาย จุดเชื่อมต่อ หรือเกตเวย์อยู่ห่างจากผนังภายนอกและหน้าต่าง
- ปิดเราเตอร์ไร้สาย จุดเชื่อมต่อ หรือเกตเวย์ เมื่อไม่ใช้ (ในกลางคืน หรือวันหยุด)
- ใช้รหัสผ่านที่เดายาก ซึ่งมีความยาวอย่างน้อย 8 อักขระ รวมตัวอักษรและตัวเลขเพื่อหลีกเลี่ยงคำพื้นฐานที่สามารถพบได้ในพจนานุกรม

การตั้งค่าขั้นสูง

หลังจากติดตั้งบริดจ์โดยทำตามขั้นตอนในที่ใส่ซีดีแล้ว บริดจ์จะพร้อมให้ใช้งาน หากคุณต้องการเปลี่ยนแปลงการตั้งค่าขั้นสูงของเราเตอร์ ให้ใช้ยูทิลิตีของบริดจ์บนเบราเซอร์ ส่วนนี้จะอธิบายถึงแต่ละเว็บเพจของยูทิลิตีและฟังก์ชันการทำงานหลักของแต่ละเพจ คุณสามารถเข้าถึงยูทิลิตีได้ผ่านเว็บเบราเซอร์ในคอมพิวเตอร์ที่มีการเชื่อมต่อกับบริดจ์

ยูทิลิตีบนเบราเซอร์มีแท็บหลัก ดังนี้ การติดตั้ง (Setup), ระบบไร้สาย (Wireless), การดูแลระบบ (Administration) และสถานะ (Status) แท็บเพิ่มเติมต่างๆ จะพร้อมใช้งานหลังจากคุณคลิกที่แท็บใดแท็บหนึ่งในแท็บหลัก

วิธีการเข้าใช้ยูทิลิตีบนเบราว์เซอร์

ใช้เว็บเบราเซอร์ในการเข้าใช้ยูทิลิตีบนเบราว์เซอร์

หากบริดจ์เชื่อมต่อกับเครือข่ายด้วยเซิร์ฟเวอร์ DHCP (โดยปกติจะเป็นเราเตอร์เครือข่าย) บริดจ์จะได้รับ IP แอดเดรสจาก DHCP หากไม่มีเซิร์ฟเวอร์ DHCP บริดจ์จะใช้ IP แอดเดรสดีฟอลต์แบบสแตติก คือ **169.254.1.250** (หากคุณตั้งค่า IP แอดเดรสแบบสแตติกถาวรบนบริดจ์ผ่านทางยูทิลิตีบนเบราว์เซอร์ ให้ป้อน IP แอดเดรสแบบสแตติกแทน)

หมายเหตุ
หากคุณไม่ทราบ IP แอดเดรสของบริดจ์คุณจะสามารถพบได้ในตารางข้อมูลไคลเอนต์ DHCP ของเราเตอร์ของคุณ (โปรดดูเอกสารประกอบสำหรับเราเตอร์ของคุณ)

หากคุณไม่สามารถค้นหาที่อยู่ IP ของบริดจ์ คุณสามารถรีเซ็ตบริดจ์โดยกดปุ่ม **Reset** บนบริดจ์ค้างไว้ประมาณ 5 วินาที โดยใช้คลิปหนีบกระดาษที่ดัดให้ตรง นี่จะทำให้บริดจ์กลับไปที่ค่าดีฟอลต์จากโรงงาน บริดจ์จะเรียก IP แอดเดรสจากเซิร์ฟเวอร์ DHCP (โดยปกติจะเป็นเราเตอร์เครือข่าย) หากไม่พบเซิร์ฟเวอร์ DHCP บริดจ์จะใช้ IP แอดเดรสแบบสแตติกที่เป็นค่าดีฟอลต์ **169.254.1.250** จนกว่าจะตรวจพบเซิร์ฟเวอร์ DHCP และมีการกำหนด IP แอดเดรสแบบไดนามิก

หากบริดจ์ไม่เชื่อมโยงกับเราเตอร์ และใช้ค่าดีฟอลต์จากโรงงาน ให้เชื่อมต่อคอมพิวเตอร์กับบริดจ์โดยใช้การเชื่อมต่อ Ethernet เพื่อเข้าใช้ยูทิลิตีบนเว็บ คุณจะต้องตั้งค่าการเชื่อมต่อ Ethernet บนคอมพิวเตอร์ด้วย IP แอดเดรสแบบสแตติก และซับเน็ตมาส์ก

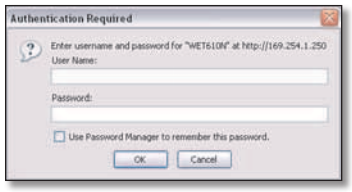
ควรตั้ง IP แอดเดรสของอะแดปเตอร์ Ethernet ของคุณไว้ที่ IP แอดเดรสที่ระบุได้

1. ในฟิลด์ *IP แอดเดรส* ให้ป้อน **169.254.x.y** (ควรแทน x ด้วยตัวเลขระหว่าง 1 - 254 และควรแทน y ด้วยตัวเลขระหว่าง 0 - 255)
2. ในฟิลด์ *ซับเน็ตมาส์ก* ให้ป้อน **255.255.0.0**

หมายเหตุ
ในขั้นตอนการกำหนด IP แอดเดรสแบบสแตติกให้กับ อะแดปเตอร์ Ethernet บนคอมพิวเตอร์ของคุณ แตกต่างกันไปตามระบบปฏิบัติการ สำหรับคำแนะนำ โปรดดูเอกสารวิธีใช้ของระบบปฏิบัติการที่ระบุ

หลังจากคุณได้กำหนดอะแดปเตอร์ Ethernet ด้วย IP แอดเดรสแบบสแตติกแล้ว ให้เปิดเว็บเบราเซอร์ของคุณ และป้อน IP แอดเดรสของอะแดปเตอร์ (ค่าดีฟอลต์ คือ **169.254.1.250**)ในฟิลด์ *Address* (แอดเดรส) กด **Enter**

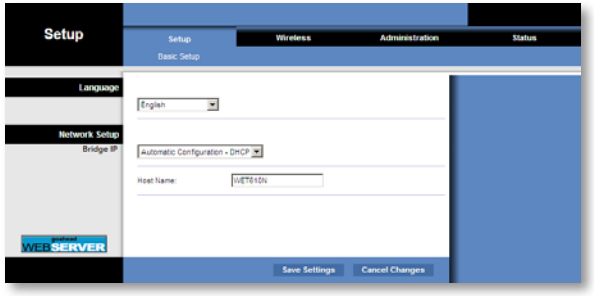
หน้าจอร้องขอรหัสผ่านจะปรากฏขึ้น (ผู้ใช้ที่ไม่ได้ใช้ Windows XP จะเห็นหน้าจอที่คล้ายคลึงกัน) เว้นฟิลด์ *User name* (ชื่อผู้ใช้) ให้ว่างไว้ ป้อนรหัสผ่านที่คุณตั้งค่าไว้ระหว่างใช้ซอฟต์แวร์การตั้งค่า (หากคุณไม่ได้สร้างรหัสผ่านใหม่ได้ ให้ใช้รหัสผ่านที่เป็นค่าดีฟอลต์ ซึ่งก็คือ **admin** (คุณสามารถตั้งค่ารหัสผ่านใหม่ได้จากหน้าจอ *Administration (การดูแลระบบ) > Management (การจัดการ)* คลิก **OK** (ตกลง) เพื่อดำเนินการต่อ

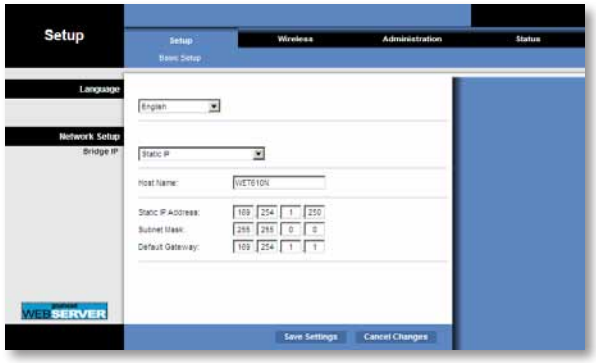


หมายเหตุ
หากหน้าจอร้องขอรหัสผ่านไม่ปรากฏขึ้น โปรดรอซักครู่และลองอีกครั้ง

Setup (การตั้งค่า) > Basic Setup (การตั้งค่าพื้นฐาน)

หน้าจอแรกที่จะปรากฏขึ้นคือหน้าจอ *Basic Setup* (การตั้งค่าพื้นฐาน) ใช้หน้าจอนี้เปลี่ยนภาษาของยูทิลิตี้บนเบราว์เซอร์ หรือเพื่อเปลี่ยนสายขอ บริดจ์และการตั้งค่าเครือข่าย Ethernet





Language (ภาษา)

Language (ภาษา) ใช้เพื่อตั้งค่าภาษาที่แสดงโดยยูทิลิตีบนเบราว์เซอร์ เลือกภาษาที่ต้องการจากเมนูดรอปดาวน์

การตั้งค่าเครือข่าย

ส่วนนี้จะกำหนดว่าจะได้รับ IP แอดเดรสของบริดจ์จากเซิร์ฟเวอร์ DHCP โดยอัตโนมัติ เช่น จากเราเตอร์เครือข่ายของคุณ (Automatic Configuration (การตั้งค่าอัตโนมัติ) - DHCP) หรือจะตั้งด้วยตนเอง (IP แบบสแตติก)

Bridge IP (บริดจ์ IP) หากเครือข่ายของคุณมีเซิร์ฟเวอร์ DHCP เช่น เราเตอร์เครือข่ายของคุณ กำหนด IP แอดเดรสให้กับอุปกรณ์เครือข่ายของคุณแล้วให้ใช้ค่าดีฟอลต์ **Automatic Configuration - DHCP**(การตั้งค่าอัตโนมัติ - DHCP) บริดจ์จะเรียก IP แอดเดรสจากเซิร์ฟเวอร์ DHCP (โดยปกติจะเป็นเราเตอร์เครือข่าย) หากไม่พบเซิร์ฟเวอร์ DHCP เมื่อนั้น บริดจ์จะใช้ IP แอดเดรสแบบสแตติกที่เป็นค่าดีฟอลต์ **169.254.1.250**จนกว่าจะตรวจพบเซิร์ฟเวอร์ DHCP และมีการกำหนด IP แอดเดรสแบบไดนามิก

หากคุณต้องการตั้งค่า IP แอดเดรสแบบสแตติกถาวรสำหรับบริดจ์ ให้เลือก **Static IP** (IP แบบสแตติก)

หากคุณเลือก Static IP (IP แบบสแตติก) ให้กรอกข้อมูลในฟิลด์ต่อไปนี้

- **Static IP Address (IP แอดเดรสแบบสแตติก)** ป้อน IP แอดเดรสที่ไม่ซ้ำกัน ซึ่งจะถูกใช้เพื่อเข้าถึงยูทิลิตีบนเบราเซอร์
- **Subnet Mask (ซับเน็ตมาส์ก)** ป้อนซับเน็ตมาส์กของเครือข่ายแบบใช้สายเชื่อมต่อของคุณ
- **Default Gateway (เกตเวย์ดีฟอลต์)** ป้อน IP แอดเดรสของเกตเวย์ดีฟอลต์สำหรับเครือค่ายของคุณ (โดยส่วนใหญ่แล้ว นี่คือเราเตอร์ของคุณ)

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือ คลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

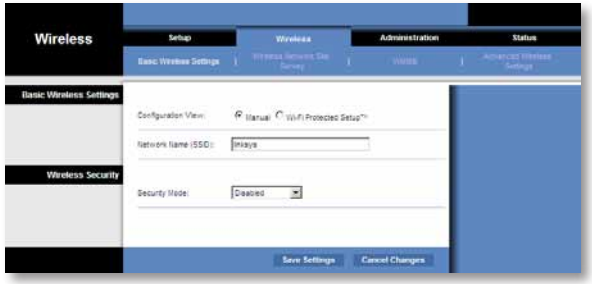
Wireless (ระบบไร้สาย) > Basic Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน)

ใช้หน้าจอ *Basic Wireless Settings* (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน) เพื่อตั้งค่าเครือข่ายไร้สายและการรักษาความปลอดภัยขั้นพื้นฐานของบริดจ์

การตั้งค่าบริดจ์ทำได้สองวิธี ได้แก่ การตั้งค่าด้วยตนเอง และการตั้งค่าแบบป้องกัน Wi-Fi Wi-Fi Protected Setup (การตั้งค่าแบบป้องกัน Wi-Fi) คือคุณสมบัติที่ช่วยให้คุณตั้งค่าเครือข่ายไร้สายของคุณได้ง่ายขึ้น หากเราเตอร์เครือข่ายของคุณสนับสนุน Wi-Fi Protected Setup และใช้การรักษาความปลอดภัย WPA หรือ WPA2 คุณสามารถใช้ Wi-Fi Protected Setup เชื่อมต่อบริดจ์ได้โดยอัตโนมัติ

Configuration View (มุมมองการกำหนดค่า) ในการกำหนดค่าเครือข่ายไร้สายของคุณด้วยตนเอง ให้เลือก **Manual**(กำหนดเอง) โปรดดูที่ **Basic Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน)**, **หน้า 8** หากต้องการใช้การตั้งค่าแบบป้องกัน Wi-Fi ให้เลือก **Wi-Fi Protected Setup** (การตั้งค่าแบบป้องกัน Wi-Fi) โปรดดูที่ **Wi-Fi Protected Setup (การตั้งค่าแบบป้องกัน Wi-Fi)**, **หน้า 9**

Basic Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน)



Network Name (SSID) (ชื่อเครือข่าย (SSID)) คือชื่อเครือข่ายที่ใช้จุดเชื่อมต่อในเครือข่ายไร้สายร่วมกันทั้งหมด SSID สำหรับอุปกรณ์ทั้งหมดในเครือข่ายไร้สายจะต้องเหมือนกัน ชื่อนี้จะจำแนกตัวพิมพ์เล็กและตัวพิมพ์ใหญ่และจะต้องมีความยาวไม่เกิน 32 อักขระ (ใช้อักขระใดบนแป้นพิมพ์ก็ได้) ตรวจสอบให้แน่ใจว่าการตั้งค่านี้ตรงกับการตั้งค่าเราเตอร์ไร้สายและจุดเชื่อมต่อของคุณ เพื่อเพิ่มการรักษาความปลอดภัย คุณควรเปลี่ยน SSID ดีฟอลต์ (**linksys**) เป็นชื่ออื่นที่ไม่ซ้ำกัน

Wireless Security (การรักษาความปลอดภัยแบบไร้สาย)

บริดจ์สนับสนุนตัวเลือกการรักษาความปลอดภัยแบบไร้สาย ดังนี้ WPA Personal, WPA2 Personal และ WEP WPA (Wi-Fi Protected Access) และ WPA2 เป็นวิธีการรักษาความปลอดภัยที่ระดับสูงกว่า WEP (Wired Equivalent Privacy) สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยไร้สาย โปรดดูที่ "Wireless Security Checklist (รายการตรวจสอบการรักษาความปลอดภัยไร้สาย)", หน้า 4

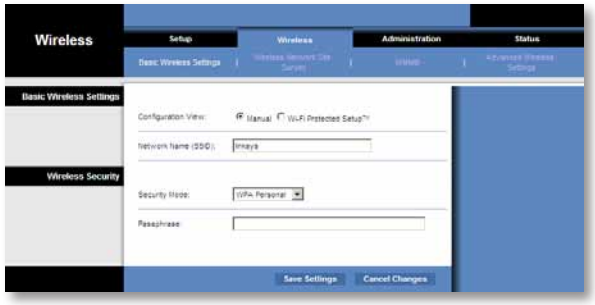
Security Mode (โหมดการรักษาความปลอดภัย)

เลือกวิธีการรักษาความปลอดภัยสำหรับเครือข่ายไร้สายของคุณ หากคุณไม่ต้องการใช้การรักษาความปลอดภัยไร้สาย ให้ใช้ตามค่าดีฟอลต์ **Disabled** (ปิดใช้งาน)

หมายเหตุ
โปรดจำไว้ว่าแต่ละอุปกรณ์ในเครือข่ายไร้สายของคุณ ต้องใช้วิธีการรักษาความปลอดภัยและรหัสผ่าน/คีย์เดียวกัน มิฉะนั้นอุปกรณ์ไร้สายจะสื่อสารระหว่างกันไม่ได้

WPA Personal

WPA เป็นมาตรฐานการรักษาความปลอดภัยที่สูงกว่าการเข้ารหัส WEP



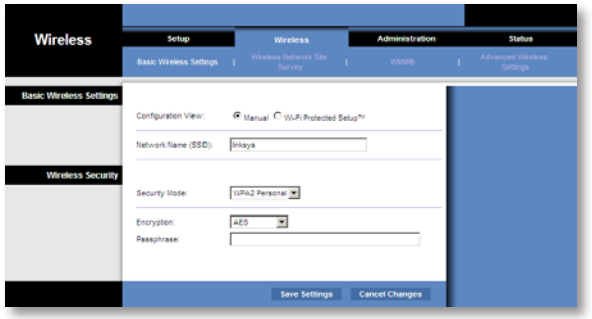
Encryption (การเข้ารหัส) WPA สนับสนุนวิธีการเข้ารหัส TKIP พร้อมด้วยคีย์การเข้ารหัสแบบไดนามิก

Passphrase (รหัสผ่าน) ป้อนคีย์ที่ใช้ร่วมกันโดย บริดจ์และเราเตอร์ไร้สายหรือจุดเชื่อมต่อของคุณ คีย์จะต้องมีอักขระ 8-63 ตัว

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

WPA2 Personal

WPA2 เป็นรุ่นที่ปลอดภัยและขั้นสูงกว่าของ WPA



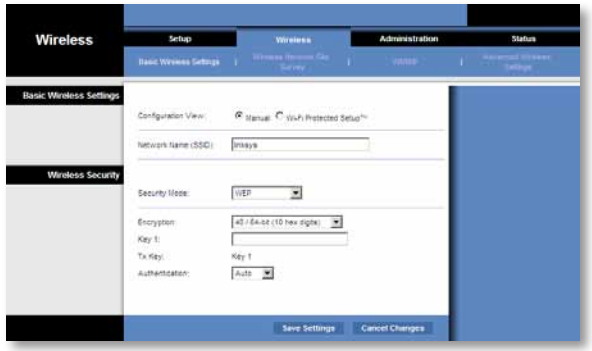
Encryption (การเข้ารหัส) WPA2 สนับสนุนการเข้ารหัส 2 วิธี คือ TKIP และ AES พร้อมด้วยคีย์การเข้ารหัสแบบไดนามิก เลือกวิธีการเข้ารหัส **AES** หรือ **TKIP หรือ AES** วิธีการที่เป็นค่าดีฟอลต์คือ **AES**

Passphrase (รหัสผ่าน) ป้อนคีย์ที่ใช้ร่วมกันโดย บริดจ์และเราเตอร์ไร้สายหรือจุดเชื่อมต่อ คีย์จะต้องมีอักขระ 8-63 ตัว

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

WEP

WEP คือวิธีการเข้ารหัสพื้นฐาน ซึ่งไม่ปลอดภัยเท่ากับ WPA หรือ WPA2



Encryption (การเข้ารหัส) เลือกระดับของการเข้ารหัส WEP **40/64 bits (10 hex digits) (40/64 บิต (10 เลขฐานสิบหก))** หรือ **(40/64 บิต (10 เลขฐานสิบหก))** ค่าดีฟอลต์คือ **40/64 bits (10 hex digits) (40/64 บิต (10 เลขฐานสิบหก))**

Key 1 (คีย์ 1) ป้อนคีย์ WEP สำหรับเครือข่ายของคุณ

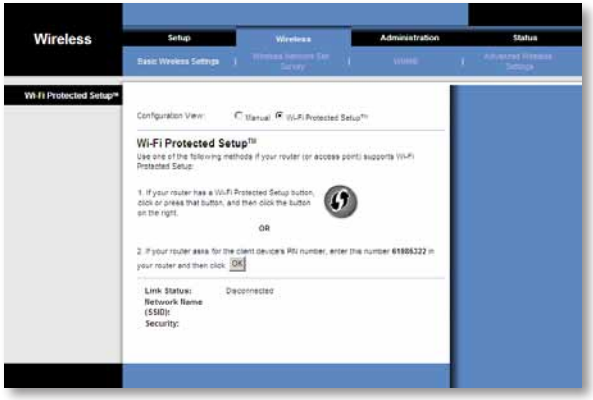
Tx Key (คีย์ TX) **Key 1** เป็นคีย์ส่งข้อมูลที่ถูกใช้โดย บริดจ์

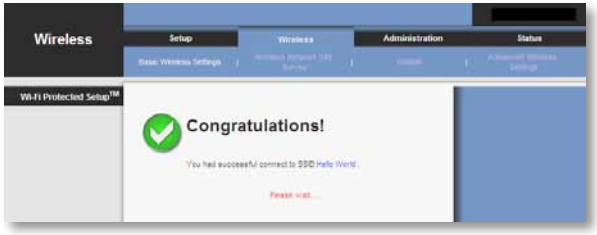
Authentication (การตรวจสอบความถูกต้อง) ค่าดีฟอลต์คือ **Auto** (อัตโนมัติ) ซึ่งอนุญาตให้มีการใช้การตรวจสอบความถูกต้องของระบบเปิดหรือคีย์ที่ใช้ร่วมกัน เลือก **Open** (เปิด) เพื่อใช้การตรวจสอบความถูกต้องของระบบเปิด ผู้ส่งและผู้รับจะต้องไม่ใช้คีย์ WEP เพื่อตรวจสอบความถูกต้อง เลือก **Shared Key** (คีย์ที่ใช้ร่วมกัน) เพื่อใช้การตรวจสอบความถูกต้องของคีย์ที่ใช้ร่วมกัน ผู้ส่งและผู้รับจะใช้คีย์ WEP เพื่อตรวจสอบความถูกต้อง

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

Wi-Fi Protected Setup (การตั้งค่าแบบป้องกัน Wi-Fi)

คุณสามารถทำได้ 2 วิธี ใช้วิธีที่เหมาะสมกับเราเตอร์ที่คุณกำลังใช้อยู่





วิธีที่ 1

ใช้วิธีนี้หากเราเตอร์ของคุณของคุณมีปุ่ม Wi-Fi Protected Setup (การตั้งค่าแบบป้องกัน Wi-Fi)

1. คลิกหรือกดปุ่ม **Wi-Fi Protected Setup** (การตั้งค่าแบบป้องกัน Wi-Fi) บนเราเตอร์
2. ภายใน 2 นาที ให้คลิกปุ่ม **Wi-Fi Protected Setup** บนหน้าจอ *Wi-Fi Protected Setup* (การตั้งค่าแบบป้องกัน Wi-Fi) ของบริดจ์
3. หลังจากบริดจ์ถูกตั้งค่าแล้ว ให้คลิก **Close**(ปิด)

หน้าจอ *Wi-Fi Protected Setup* แสดง Link Status (สถานะการเชื่อมโยง), Network Name (SSID) (ชื่อเครือข่าย (SSID)) และวิธีการรักษาความปลอดภัย

วิธีที่ 2

ใช้วิธีนี้หากเราเตอร์ของคุณร้องขอหมายเลข PIN ของบริดจ์

1. บนหน้าจอ *Wi-Fi Protected Setup* ของ **เราเตอร์** ให้ป้อนหมายเลข PIN บนหน้าจอ *Wi-Fi Protected Setup* ของ **บริดจ์** จากนั้น คลิก **Register** (ลงทะเบียน) หรือปุ่มที่ต้องการ (แสดงอยู่บนป้ายที่ด้านใต้ของบริดจ์เช่นกัน)
2. บนหน้าจอ *Wi-Fi Protected Setup* ของ **บริดจ์** ให้คลิก **OK** (ตกลง)
3. หลังจากบริดจ์ถูกตั้งค่าแล้ว ให้คลิก **Close**(ปิด)

หน้าจอ *Wi-Fi Protected Setup* แสดง Link Status (สถานะการเชื่อมโยง), Network Name (SSID) (ชื่อเครือข่าย (SSID)) และวิธีการรักษาความปลอดภัย

Wireless (ระบบไร้สาย) > Wireless Network Site Survey (แบบสำรวจไซต์เครือข่ายไร้สาย)

คลิกแท็บ **Wireless Network Site Survey** เพื่อเริ่มการสำรวจไซต์ หน้าจอ *Wireless Network Site Survey* แสดงรายการของเครือข่ายไร้สายที่ถูกตรวจพบโดยบริดจ์



Wireless Network Site Survey (แบบสำรวจไซต์เครือข่ายไร้สาย)

Number of Wireless Networks (จำนวนเครือข่ายไร้สาย) แสดงจำนวนของเครือข่ายไร้สายที่ถูกตรวจพบโดยบริดจ์

เลือก เพื่อเชื่อมต่อกับเครือข่ายไร้สาย คลิก **Select**(เลือก) จากนั้นคลิก **Connect** (เชื่อมต่อ)

Wireless Network Name (ชื่อเครือข่ายไร้สาย) แสดงชื่อเครือข่าย หรือ SSID ของเครือข่ายไร้สาย

GHz แสดงความถี่วิทยุของเครือข่ายไร้สาย

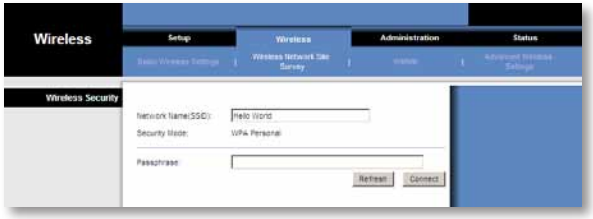
Signal (สัญญาณ) แสดงเปอร์เซ็นต์ความแรงของสัญญาณ ความแรงของสัญญาณสูงสุด 100% และต่ำสุดที่ 0%

Security (การรักษาความปลอดภัย) หาก เครือข่ายสนับสนุน Wi-Fi Protected Setup ไอคอน Wi-Fi Protected Setup จะถูกแสดงอยู่ แสดงวิธีการรักษาความปลอดภัยระบบไร้สายที่เราเตอร์ใช้

คลิก **Refresh** (รีเฟรช) เพื่ออัปเดตข้อมูลบนหน้าจอ

หลังจากที่คุณเลือกเครือข่ายแล้ว ให้คลิก **Connect**(เชื่อมต่อ) หน้าจอใหม่จะปรากฏขึ้น ทำตามคำแนะนำสำหรับวิธีการรักษาความปลอดภัยของเครือข่ายของคุณ

WPA



Network Name (SSID) (ชื่อเครือข่าย (SSID)) แสดงชื่อเครือข่ายที่คุณเลือกโดยอัตโนมัติ

Security Mode (โหมดการรักษาความปลอดภัย) WPA Personal จะถูกแสดงโดยอัตโนมัติ

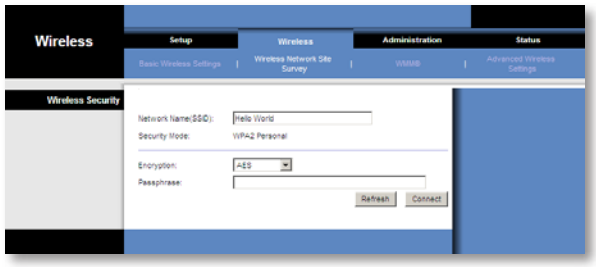
Encryption (การเข้ารหัส) WPA สนับสนุนวิธีการเข้ารหัส TKIP พร้อมด้วยคีย์การเข้ารหัสแบบไดนามิก

Passphrase (รหัสผ่าน) ป้อนคีย์ที่ใช้ร่วมกันโดย บริดจ์และเราเตอร์ไร้สายหรือจุดเชื่อมต่อ คีย์จะต้องมีอักขระ 8-63 ตัว

คลิก **Refresh** (รีเฟรช) เพื่ออัปเดตข้อมูลบนหน้าจอ

หลังจากที่คุณป้อนการตั้งค่าการการรักษาความปลอดภัยแล้ว ให้คลิก **Connect** (เชื่อมต่อ)

WPA2



Network Name (SSID) (ชื่อเครือข่าย (SSID)) แสดงชื่อเครือข่ายที่คุณเลือกโดยอัตโนมัติ

Security Mode (โหมดการรักษาความปลอดภัย) WPA Personal จะถูกแสดงโดยอัตโนมัติ

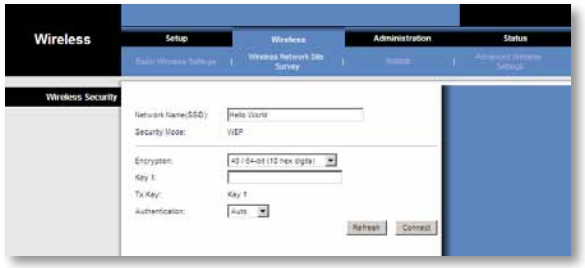
Encryption (การเข้ารหัส) WPA2 สนับสนุนการเข้ารหัส 2 วิธี คือ TKIP และ AES พร้อมด้วยคีย์การเข้ารหัสแบบไดนามิก เลือกวิธีการเข้ารหัส **AES** หรือ **TKIP หรือ AES**

Passphrase (รหัสผ่าน) ป้อนคีย์ที่ใช้ร่วมกันโดย บริดจ์และเราเตอร์ไร้สายหรือจุดเชื่อมต่อ คีย์จะต้องมีอักขระ 8-63 ตัว

คลิก **Refresh** (รีเฟรช) เพื่ออัปเดตข้อมูลบนหน้าจอ

หลังจากที่คุณป้อนการตั้งค่าการการรักษาความปลอดภัยแล้ว ให้คลิก **Connect** (เชื่อมต่อ)

WEP



Network Name (SSID) (ชื่อเครือข่าย (SSID)) แสดงชื่อเครือข่ายที่คุณเลือกโดยอัตโนมัติ

Security Mode (โหมดการรักษาความปลอดภัย) WPA จะถูกแสดงโดยอัตโนมัติ

Encryption (การเข้ารหัส) เลือกระดับของการเข้ารหัส WEP **40/64 bits (10 hex digits)** (40/64 บิต (10 เลขฐานสิบหก)) หรือ **104/128 bits (26 hex digits)**(104/128 บิต (26 เลขฐานสิบหก))

Key 1 (คีย์ 1) ป้อนคีย์ WEP สำหรับเครือข่ายของคุณ

Tx Key (คีย์ TX) **Key 1** เป็นคีย์ส่งข้อมูลที่ถูกใช้โดย บริดจ์

Authentication (การตรวจสอบความถูกต้อง) ค่าดีฟอลต์คือ **Auto**(อัตโนมัติ) ซึ่งอนุญาตให้มีการใช้การตรวจสอบความถูกต้องของระบบเปิดหรือคีย์ที่ใช้ร่วมกัน เลือก **Open** (เปิด) เพื่อใช้การตรวจสอบความถูกต้องของระบบเปิด ผู้ส่งและผู้รับจะต้องไม่ใช้คีย์ WEP เพื่อตรวจสอบความถูกต้อง เลือก **Shared Key** (คีย์ที่ใช้ร่วมกัน) เพื่อใช้การตรวจสอบความถูกต้องของคีย์ที่ใช้ร่วมกัน ผู้ส่งและผู้รับจะใช้คีย์ WEP เพื่อตรวจสอบความถูกต้อง

คลิก **Refresh** (รีเฟรช) เพื่ออัปเดตข้อมูลบนหน้าจอ

หลังจากที่คุณป้อนการตั้งค่าการการรักษาความปลอดภัยแล้ว ให้คลิก **Connect** (เชื่อมต่อ)

Wireless (ระบบไร้สาย) > WMM®

ตั้งค่า Wireless MultiMedia (WMM) WMM จัดลำดับแพคเก็ตโดยขึ้นอยู่กับโหมดการเข้าถึงตามลำดับ (ประเภททราฟฟิก) ได้แก่ พื้นหลัง, Best Effort, ภาพหรือเสียง ควรปรับการตั้งค่านี้โดยผู้ดูแลระบบที่เชี่ยวชาญเท่านั้น เนื่องจากหากตั้งค่าผิดจะทำให้ประสิทธิภาพการทำงานของเครือข่ายไร้สายด้อยลง



หมายเหตุ
การตั้งค่าบนหน้าจอ *WMM* ได้รับการออกแบบเพื่อผู้ใช้ขั้นสูงเท่านั้น

WMM

Access Mode (โหมดการเข้าใช้)

คุณสามารถกำหนดการตั้งค่าที่ต่างกันให้กับ 4 โหมดที่มีอยู่ เลือกโหมดที่คุณต้องการตั้งค่าดังนี้ **Background**(พื้นหลัง), **Best Effort**, **Video** (ภาพ) หรือ **Voice** (เสียง) ทำตามคำแนะนำสำหรับโหมดที่คุณเลือก

Background (พื้นหลัง)

Use Aggregation (ใช้การรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ Media Access Control (MAC) จะตั้งต่าเซสชัน Add Block Acknowledgement (ADDBA) หรือไม่ ค่าดีฟอลต์คือ **No**(ไม่) เลือก **Yes** (ใช่) เพื่อเปิดการใช้งานตัวเลือกนี้

Accept Aggregation (ยอมรับการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ MAC จะยอมรับการร้องขอจาก ADDBA หรือไม่ ค่าดีฟอลต์คือ **Yes**(ใช่) เลือก **No** (ไม่) เพื่อปิดการใช้งานตัวเลือกนี้

Max. Number of Packets in Aggregation (จำนวนสูงสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ต(เฟรมย่อย) ในการรวมกลุ่ม มีระยะ **0** - **7** ค่าดีฟอลต์คือ **7**

Max. Aggregation Size (ขนาดการรวมกลุ่มสูงสุด) ตัวเลือกนี้จะกำหนดขนาดสูงสุดของการรวมกลุ่ม (เป็นไบต์) มีระยะ **0** - **16000** ค่าดีฟอลต์คือ **12000**

Timeout Internal (การหมดเวลาภายใน) ตัวเลือกนี้จะกำหนดระยะหมดเวลาที่การรวมกลุ่มควรจะถูกปิดด้วย "closing condition" ก่อนที่จะถูกปิดด้วยตัวจับเวลา มีระยะ **0** - **100** ms ค่าดีฟอลต์คือ **3**

Min. Size of Packet in Aggregation (ขนาดต่ำสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดขนาดต่ำสุดของแพคเก็ต (เป็นไบต์) ที่ถูกรวบรวมในการรวมกลุ่ม มีระยะ **0** - **1500** ค่าดีฟอลต์คือ **10**

ADDBA Timeout (การหมดเวลาของ ADDBA) ตัวเลือกนี้จะกำหนดระยะเวลาหลังจากการติดตั้ง ADDBA สิ้นสุด หากไม่มีการแลกเปลี่ยนเฟรมภายในระยะเวลานี้ โดยข้อตกลง Block Acknowledgement (ACK) มีระยะ **0** - **65535** ms ค่าดีฟอลต์คือ **0**ซึ่งจะปิดการใช้งานการหมดเวลา

Aggregation Window Size (ขนากหน้าต่างการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ตที่ถูกส่งโดยไม่ได้รับ ACK มีระยะ **0** - **64** ค่าดีฟอลต์คือ **64**

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

Best Effort

Use Aggregation (ใช้การรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ Media Access Control (MAC) จะตั้งค่าเซสชัน Add Block Acknowledgement (ADDBA) หรือไม่ ค่าดีฟอลต์คือ **Yes**(ใช่) เลือก **No** (ไม่) เพื่อปิดการใช้งานตัวเลือกนี้

Accept Aggregation (ยอมรับการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ MAC จะยอมรับการร้องขอจาก ADDBA หรือไม่ ค่าดีฟอลต์คือ **Yes**(ใช่) เลือก **No** (ไม่) เพื่อปิดการใช้งานตัวเลือกนี้

Max. Number of Packets in Aggregation (จำนวนสูงสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ต(เฟรมย่อย) ในการรวมกลุ่ม มีระยะ **0** - **10** ค่าดีฟอลต์คือ **10**

Max. Aggregation Size (ขนาดการรวมกลุ่มสูงสุด) ตัวเลือกนี้จะกำหนดขนาดสูงสุดของการรวมกลุ่ม (เป็นไบต์) มีระยะ **0** - **20000** ค่าดีฟอลต์คือ **16000**

Timeout Internal (การหมดเวลาภายใน) ตัวเลือกนี้จะกำหนดระยะหมดเวลาที่การรวมกลุ่มควรจะถูกปิดด้วย "closing condition" ก่อนที่จะถูกปิดด้วยตัวจับเวลา มีระยะ **0** - **100** ms ค่าดีฟอลต์คือ **3**

Min. Size of Packet in Aggregation (ขนาดต่ำสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดขนาดต่ำสุดของแพคเก็ต (เป็นไบต์) ที่ถูกรวบรวมในการรวมกลุ่ม มีระยะ **0** - **1500** ค่าดีฟอลต์คือ **10**

ADDBA Timeout (การหมดเวลาของ ADDBA) ตัวเลือกนี้จะกำหนดระยะเวลาหลังจากการติดตั้ง ADDBA สิ้นสุด หากไม่มีการแลกเปลี่ยนเฟรมภายในระยะเวลานี้ โดยข้อตกลง Block Acknowledgement (ACK) มีระยะ **0** - **65535** ms ค่าดีฟอลต์คือ **0**ซึ่งจะปิดการใช้งานการหมดเวลา

Aggregation Window Size (ขนากหน้าต่างการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ตที่ถูกส่งโดยไม่ได้รับ ACK มีระยะ **0** - **64** ค่าดีฟอลต์คือ **64**

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

Video (ภาพ)

Use Aggregation (ใช้การรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ Media Access Control (MAC) จะตั้งค่าเซสชัน Add Block Acknowledgement (ADDBA) หรือไม่ ค่าดีฟอลต์คือ **Yes**(ใช่) เลือก **No** (ไม่) เพื่อปิดการใช้งานตัวเลือกนี้

Accept Aggregation (ยอมรับการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ MAC จะยอมรับการร้องขอจาก ADDBA หรือไม่ ค่าดีฟอลต์คือ **Yes**(ใช่) เลือก **No** (ไม่) เพื่อปิดการใช้งานตัวเลือกนี้

Max. Number of Packets in Aggregation (จำนวนสูงสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ต(เฟรมย่อย) ในการรวมกลุ่ม มีระยะ **0** - **7** ค่าดีฟอลต์คือ **7**

Max. Aggregation Size (ขนาดการรวมกลุ่มสูงสุด) ตัวเลือกนี้จะกำหนดขนาดสูงสุดของการรวมกลุ่ม (เป็นไบต์) มีระยะ **0** - **16000** ค่าดีฟอลต์คือ **12000**

Timeout Internal (การหมดเวลาภายใน) ตัวเลือกนี้จะกำหนดระยะหมดเวลาที่การรวมกลุ่มควรจะถูกปิดด้วย "closing condition" ก่อนที่จะถูกปิดด้วยตัวจับเวลา มีระยะ **0** - **100** ms ค่าดีฟอลต์คือ **3**

Min. Size of Packet in Aggregation (ขนาดต่ำสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดขนาดต่ำสุดของแพคเก็ต (เป็นไบต์) ที่ถูกรวบรวมในการรวมกลุ่ม มีระยะ **0** - **1500** ค่าดีฟอลต์คือ **10**

ADDBA Timeout (การหมดเวลาของ ADDBA) ตัวเลือกนี้จะกำหนดระยะเวลาหลังจากการติดตั้ง ADDBA สิ้นสุด หากไม่มีการแลกเปลี่ยนเฟรมภายในระยะเวลานี้ โดยข้อตกลง Block Acknowledgement (ACK) มีระยะ **0** - **65535** ms ค่าดีฟอลต์คือ **0**ซึ่งจะปิดการใช้งานการหมดเวลา

Aggregation Window Size (ขนากหน้าต่างการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ตที่ถูกส่งโดยไม่ได้รับ ACK มีระยะ **0** - **64** ค่าดีฟอลต์คือ **64**

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

Voice (เสียง)

Use Aggregation (ใช้การรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ Media Access Control (MAC) จะตั้งค่าเซสชัน Add Block Acknowledgement (ADDBA) หรือไม่ ค่าดีฟอลต์คือ **Yes**(ใช่) เลือก **No** (ไม่) เพื่อปิดการใช้งานตัวเลือกนี้

Accept Aggregation (ยอมรับการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดว่าเลเยอร์ MAC จะยอมรับการร้องขอจาก ADDBA หรือไม่ ค่าดีฟอลต์คือ **Yes**(ใช่) เลือก **No** (ไม่) เพื่อปิดการใช้งานตัวเลือกนี้

Max. Number of Packets in Aggregation (จำนวนสูงสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ต(เฟรมย่อย) ในการรวมกลุ่ม มีระยะ **0** - **2** ค่าดีฟอลต์คือ **2**

Max. Aggregation Size (ขนาดการรวมกลุ่มสูงสุด) ตัวเลือกนี้จะกำหนดขนาดสูงสุดของการรวมกลุ่ม (เป็นไบต์) มีระยะ **0** - **16000** ค่าดีฟอลต์คือ **10000**

Timeout Internal (การหมดเวลาภายใน) ตัวเลือกนี้จะกำหนดระยะหมดเวลาที่การรวมกลุ่มควรจะถูกปิดด้วย "closing condition" ก่อนที่จะถูกปิดด้วยตัวจับเวลา มีระยะ **0** - **100** ms ค่าดีฟอลต์คือ **10**

Min. Size of Packet in Aggregation (ขนาดต่ำสุดของแพคเก็ตในการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดขนาดต่ำสุดของแพคเก็ต (เป็นไบต์) ที่ถูกรวบรวมในการรวมกลุ่ม มีระยะ **0** - **1500** ค่าดีฟอลต์คือ **10**

ADDBA Timeout (การหมดเวลาของ ADDBA) ตัวเลือกนี้จะกำหนดระยะเวลาหลังจากการติดตั้ง ADDBA สิ้นสุด หากไม่มีการแลกเปลี่ยนเฟรมภายในระยะเวลานี้ โดยข้อตกลง Block Acknowledgement (ACK) มีระยะ **0** - **65535** ms ค่าดีฟอลต์คือ **0**ซึ่งจะปิดการใช้งานการหมดเวลา

Aggregation Window Size (ขนากหน้าต่างการรวมกลุ่ม) ตัวเลือกนี้จะกำหนดจำนวนสูงสุดของแพคเก็ตที่ถูกส่งโดยไม่ได้รับ ACK มีระยะ **0** - **64** ค่าดีฟอลต์คือ **64**

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

Wireless (ระบบไร้สาย) > Advanced Wireless Settings (การตั้งค่าเครือข่ายไร้สายขั้นสูง)

ตั้งค่าฟังก์ชันเครือข่ายไร้สายขั้นสูงของบริดจ์ ควรปรับการตั้งค่านี้โดยผู้ดูแลระบบที่เชี่ยวชาญเท่านั้น เนื่องจากหากตั้งค่าผิด จะทำให้ประสิทธิภาพการทำงานของเครือข่ายไร้สายด้อยลง



หมายเหตุ
การตั้งค่าบนหน้าจอ *Advanced Wireless Settings* ได้รับการออกแบบเพื่อผู้ใช้ขั้นสูงเท่านั้น

Advanced Wireless (เครือข่ายไร้สายขั้นสูง)

Use LDPC (ใช้ LDPC) Low-Density Parity-Check Code (LDPC) เปิดหรือปิดการใช้การแก้ไขข้อผิดพลาด เพื่อลดความน่าจะเป็นของการสูญเสียข้อมูลในช่องสัญญาณที่มีสัญญาณรบกวน อัลกอริทึม Rate Adaptation ปิดการเข้ารหัส LDPC โดยอัตโนมัติ เมื่อทำงานในอัตรา PHY สูง (สูงกว่า 162) หากต้องการใช้แบบแผนการแก้ไขข้อผิดพลาดขั้นสูง LDCP ให้ใช้ค่าดีฟอลต์ **Yes**(ใช่) มิฉะนั้น ให้เลือก **No**(ไม่)

ERP Protection Type (ชนิดของการป้องกัน ERP) ตัวเลือกนี้จะตั้งค่าการป้องกันแพคเก็ต OFDM แม้จะมีสถานี 802.11b ภายในเครือข่ายไร้สาย ด้วยการส่งแพคเก็ต RTS/CTS หรือ CTS2Self packets ในอัตรา 802.11b บริดจ์จะแจ้งไปยังเครือข่ายไร้สายว่าแพคเก็ต OFDM จะถูกส่ง และป้องกันแพคเก็ตในเครือข่ายไร้สาย แพคเก็ต RTS/CTS และ CTS2Self จะสร้างโอเวอร์เฮด ซึ่งอาจส่งผลให้อัตราความเร็วลดลง

ตัวเลือก RTS/CTS ให้การครอบคลุมที่ดีกว่า แต่ให้อัตราความเร็วต่ำกว่า CTS2Self เนื่องจากตัวเลือก RTS/CTS ยังรวมถึงการตอบรับจากอุปกรณ์รับสัญญาณ หากต้องการใช้ตัวเลือก RTS/CTS ให้ใช้ค่าดีฟอลต์ **RTS/CTS** ตัวเลือก None อาจทำให้เกิดความขัดแย้งระหว่างแพคเก็ต OFDM และ CCK หากต้องการใช้ตัวเลือก None ให้เลือก **None** หากต้องการใช้ตัวเลือก CTS2Self ให้เลือก **CTS2Self**

11n Protection Type (ชนิดของการป้องกัน 11n) ตัวเลือกนี้จะตั้งค่าการป้องกันอุปกรณ์ที่ไม่มี High Throughput (HT) ภายในเครือข่ายไร้สาย ในกรณีที่เราเตอร์ไร้สาย (หรือจุดเชื่อมต่อ) ตรวจพบการเชื่อมโยงของอุปกรณ์รุ่นดั้งเดิมที่ไม่มี HT เราเตอร์จะส่งสัญญาณไปยังอุปกรณ์ HT ให้ใช้กลไก RTS/CTS หรือ CTS2Self ก่อนการส่งข้อมูลแต่ละครั้ง คุณสมบัตินี้ยังสนับสนุนการป้องกันพื้นฐาน 802.11n ทั้งหมด รวมถึง MIMO

ตัวเลือก RTS/CTS ให้การครอบคลุมที่ดีกว่า แต่ให้อัตราความเร็วต่ำกว่า CTS2Self เนื่องจากตัวเลือก RTS/CTS นั้นรวมถึงการตอบรับจากอุปกรณ์รับสัญญาณด้วย หากต้องการใช้ตัวเลือก RTS/CTS ให้ใช้ค่าดีฟอลต์ **RTS/CTS** ตัวเลือก None อาจทำให้เกิดความขัดแย้งระหว่างแพคเก็ตดั้งเดิม และ HT หากต้องการใช้ตัวเลือก None ให้เลือก **None** หากต้องการใช้ตัวเลือก CTS2Self ให้เลือก **CTS2Self**

Percentage of maximal transmit power (เปอร์เซ็นต์กำลังการส่งสูงสุด) ตัวเลือกนี้จะตั้งเปอร์เซ็นต์ของกำลังการส่งสูงสุด เทียบกับการจำกัดข้อบังคับโดเมน ตัวอย่างเช่น หากข้อจำกัดโดเมนให้ส่งสัญญาณได้ถึง 20 dB ดังนั้นการตั้งเปอร์เซ็นต์ที่ 50% จะให้กำลังการส่งสูงสุดสำหรับ 10 dB เลือกเปอร์เซ็นต์ที่คุณต้องการใช้ดังนี้ **12%**, **25%**, **50%**หรือ **100%** ค่าดีฟอลต์คือ **100%**

QoS Classification Type (การจำแนกประเภท QoS) ตัวเลือกนี้จะตั้งแมป 802.1D หรือ 802.1Q จากฟิลด์ IP DSCP/TOS field ถึงลำดับ WMM (พื้นหลัง, Best Effects, ภาพ, เสียง) ให้ใช้ค่าดีฟอลต์ **802.1D**หรือเลือก **802.1Q** ซึ่งถูกใช้โดยบางสตรีม IPTV

Re-establish Ethernet connection when initiating wireless connection (การเชื่อมต่อ Ethernet ใหม่ เมื่อเริ่มการเชื่อมต่อไร้สาย) ในการเริ่มการค้นพบ DHCP จากอุปกรณ์ที่อยู่ในบริดจ์ บริดจ์จะรีเซตลิงค์ Ethernet ระหว่างบริดจ์และอุปกรณ์ทุกครั้งที่การเชื่อมต่อไร้สายเกิดขึ้น หากต้องการปิดลักษณะการทำงานนี้ ให้เลือก **No**(ไม่) มิฉะนั้นให้ใช้ค่าดีฟอลต์ **Yes**(ใช่)

คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

Administration (การดูแลระบบ) > Management (การจัดการ)

ใช้หน้าจอนี้เพื่อจัดการฟังก์ชันการทำงานเฉพาะของบริดจ์ เช่น เข้าใช้ยูทิลิตีบนเว็บ, สำรองไฟล์การตั้งค่า และรีบูต



Management (การจัดการ)

Bridge Access (การเข้าใช้บริดจ์)

ใช้รหัสผ่านเพื่อป้องกันการเข้าใช้ยูทิลิตีบนเบราว์เซอร์

Bridge Password (รหัสผ่านของบริดจ์) ป้อนรหัสผ่านใหม่สำหรับบริดจ์

Re-enter to confirm (ยืนยันรหัสผ่าน) ป้อนรหัสผ่านอีกครั้งเพื่อยืนยัน

Idle Timeout (ระยะหมดเวลาเมื่อไม่ใช้งาน) การล็อกอินจะหมดเวลาหลังจากไม่มีการใช้งานเป็นระยะเวลาที่คุณกำหนด มีระยะ **60** - **3600** วินาที ค่าดีฟอลต์คือ **600**

Web Access (การเข้าถึงเว็บ)

Access via Wireless (เข้าใช้ผ่านเครือข่ายไร้สาย) หากคุณใช้บริดจ์ในโดเมนสาธารณะที่คุณให้ผู้ใช้ภายนอกของคุณเข้าถึงแบบไร้สายได้ คุณสามารถปิดใช้งานการเข้าถึงแบบไร้สายสำหรับยูทิลิตีที่ทำงานบนเบราว์เซอร์ของบริดจ์ได้ คุณจะสามารถเข้าใช้ยูทิลิตีบนเบราว์เซอร์ผ่านการเชื่อมต่อผ่านสายเท่านั้น หากคุณปิดการตั้งค่านี้ ให้ใช้ค่าดีฟอลต์ **Enabled**(เปิดใช้งาน) เพื่ออนุญาตการเข้าใช้แบบไร้สาย สำหรับยูทิลิตีบนเบราว์เซอร์ของบริดจ์ หรือเลือก **Disabled** (ปิดใช้งาน) เพื่อบล็อคการเข้าใช้ยูทิลิตีแบบไร้สาย

Backup and Restore (การสำรองและการเรียกคืน)

Backup (สำรอง) หากต้องการสำรองไฟล์ตั้งค่าของบริดจ์ ให้คลิก **Backup Configurations** (สำรองการตั้งค่า) จากนั้นทำตามคำแนะนำบนหน้าจอ

Restore (เรียกคืน) คลิก **Browse** (เลือกดู) และเลือกไฟล์การตั้งค่า แล้วคลิก **Restore Configurations** (เรียกคืนการตั้งค่า)

System Reboot (การรีบูตระบบ)

Reboot (รีบูต) เพื่อรีบูตหรือรีสตาร์ทบริดจ์ ให้คลิก **Start to Reboot**(เริ่มรีบูต)

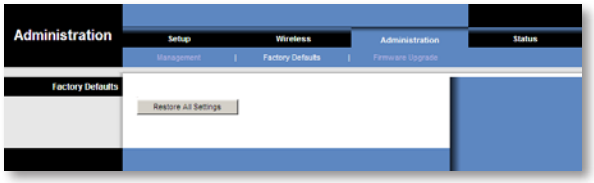
คลิก **Save Settings** (บันทึกการตั้งค่า) เพื่อนำการเปลี่ยนแปลงของคุณไปใช้ หรือคลิก **Cancel Changes** (ยกเลิกการเปลี่ยนแปลง) เพื่อยกเลิกการเปลี่ยนแปลงของคุณ

Administration (การดูแลระบบ) > Factory Defaults (ค่าดีฟอลต์จากโรงงาน)

ใช้หน้าจอนี้เรียกคืนการตั้งค่าบริดจ์ให้กลับไปเป็นค่าดีฟอลต์ได้

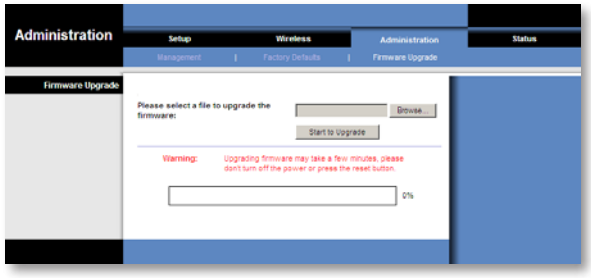
Factory Defaults (ค่าดีฟอลต์จากโรงงาน)

Restore All Settings (เรียกคืนการตั้งค่าทั้งหมด) เพื่อรีเซตการตั้งค่าบริดจ์เป็นค่าดีฟอลต์จากโรงงาน ให้คลิก **Restore All Settings**(เรียกคืนการตั้งค่าทั้งหมด) การตั้งค่าใดๆ ที่คุณบันทึกไว้จะสูญหายเมื่อมีการเรียกคืนการตั้งค่ากลับไปเป็นค่าดีฟอลต์



Administration (การดูแลระบบ) > Upgrade Firmware (อัปเกรดเฟิร์มแวร์)

ใช้ตัวเลือกนี้เพื่ออัปเกรดเฟิร์มแวร์ของบริดจ์ อย่าอัปเกรดเฟิร์มแวร์หากคุณไม่ได้มีปัญหาในการใช้งานบริดจ์ หรือเฟิร์มแวร์ใหม่ไม่มีคุณสมบัติที่คุณต้องการใช้งาน



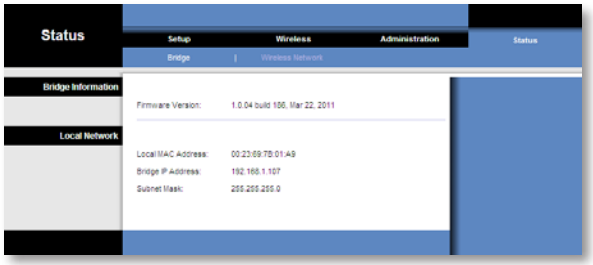
ก่อนที่จะปรับรุ่นเฟิร์มแวร์ ให้ดาวน์โหลดไฟล์อัปเกรดเฟิร์มแวร์ของบริดจ์จากเว็บไซต์ของ Linksys **www.linksys.com/support**

Upgrade Firmware (อัปเกรดเฟิร์มแวร์)

Please select a file to upgrade the firmware (โปรดเลือกไฟล์ที่จะอัปเกรดเฟิร์มแวร์) คลิก **Browse** (เรียกดู) แล้วเลือกไฟล์อัปเกรดเฟิร์มแวร์ แล้วคลิก **Start to Upgrade**(เริ่มการอัปเกรด) และทำตามคำแนะนำบนหน้าจอ

Status (สถานะ) > Bridge (บริดจ์)

แสดงสถานะปัจจุบันของบริดจ์



Bridge Information (ข้อมูลของบริดจ์)

Firmware Version (รุ่นของเฟิร์มแวร์) แสดงเฟิร์มแวร์ปัจจุบันของบริดจ์

Local Network (เครือข่ายภายใน)

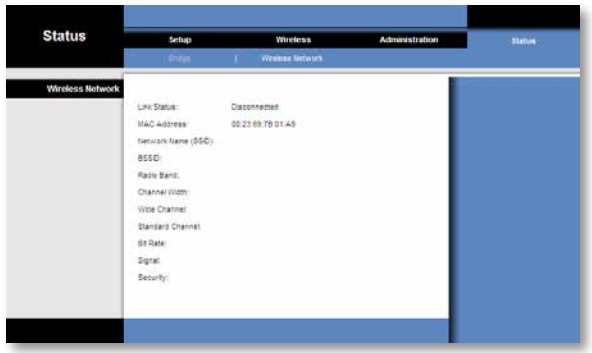
Internet MAC Address (แอดเดรส MAC บนอินเทอร์เน็ต) จะแสดงแอดเดรส MAC ของบริดจ์ที่ปรากฏต่อเครือข่าย Ethernet ภายในของคุณ

IP Address (IP แอดเดรส) จะแสดง IP แอดเดรสของบริดจ์ที่ปรากฏต่อเครือข่าย Ethernet ภายในของคุณ

Subnet Mask (ซับเน็ตมาสก์) จะแสดงซับเน็ตมาสก์ที่ตั้งค่าสำหรับเครือข่ายภายในของคุณ

Status (สถานะ) > Wireless (ระบบไร้สาย)

แสดงข้อมูลเกี่ยวกับเครือข่ายไร้สายของคุณ



Wireless (ระบบไร้สาย)

Link Status (สถานะการเชื่อมโยง) จะแสดงสถานะของการเชื่อมต่อเครือข่ายไร้สายของคุณ

MAC Address (แอดเดรส MAC) จะแสดง(แอดเดรส MAC ที่ปรากฏต่อเครือข่ายไร้สายของคุณ

Network Name (SSID) (ชื่อเครือข่าย (SSID)) แสดงชื่อเครือข่ายไร้สายหรือ SSID

BSSID แสดง MAC แอดเดรสไร้สายของเราเตอร์ที่เชื่อมต่อไร้สายอยู่

Radio Band (ความถี่วิทยุ) แสดงความถี่วิทยุของเครือข่ายไร้สาย

Channel Width (ความกว้างของช่องสัญญาณ) แสดงความกว้างของช่องสัญญาณที่ถูกใช้โดยเครือข่ายไร้สายของคุณเป็น MHz

Wide Channel (ช่องสัญญาณแบบกว้าง) แสดงช่องสัญญาณแบบกว้างโดยขึ้นอยู่กับการตั้งค่าช่องสัญญาณของเราเตอร์เครือข่ายของคุณ หากคุณเลือกช่องสัญญาณกว้าง 40MHz Channel สำหรับความถี่วิทยุของเราเตอร์ หรือการตั้งค่าความกว้างช่องสัญญาณ ดังนั้นนี่จะเป็นช่องสัญญาณ Wireless-N หลักของคุณ

Standard Channel (ช่องสัญญาณแบบมาตรฐาน) แสดงการตั้งค่าของช่องสัญญาณแบบมาตรฐาน หากคุณเลือกช่องสัญญาณกว้าง 40MHz Channel สำหรับความถี่วิทยุของเราเตอร์ หรือการตั้งค่าความกว้างช่องสัญญาณ ดังนั้นช่องสัญญาณแบบมาตรฐานจะเป็นช่องสัญญาณรองของคุณ

Bit Rate (อัตราบิต) แสดงอัตราการส่งข้อมูล

Signal (สัญญาณ) แสดงเปอร์เซ็นต์ความแรงของสัญญาณ ความแรงของสัญญาณสูงสุด 100% และต่ำสุดที่ 0%

Security (การรักษาความปลอดภัย) แสดงวิธีการรักษาความปลอดภัยของเครือข่ายไร้สายของคุณ

การแก้ไขปัญหา

WES610N/WET610N

คอมพิวเตอร์หรืออุปกรณ์เชื่อมต่อ Ethernet ผ่านสายใดๆ ไม่สามารถสื่อสารกับเราเตอร์ได้

1. การเข้าใช้ยูทิลิตีบนเบราว์เซอร์ของบริดจ์
2. บนหน้าจอ *Basic Wireless Settings* (การตั้งค่าเครือข่ายไร้สายขั้นพื้นฐาน) ตรวจสอบให้แน่ใจว่าชื่อเครือข่ายไร้สาย (SSID) ตรงกับชื่อของเครือข่ายไร้สายของคุณ
3. ตรวจสอบให้แน่ใจว่าการตั้งค่าการรักษาความปลอดภัย (WPA, WPA2 หรือ WEP) ตรงกับการตั้งค่าการรักษาความปลอดภัยของเครือข่ายไร้สายของคุณ

ต้องเปลี่ยน IP แอดเดรสของบริดจ์

หากบริดจ์เชื่อมต่อกับเครือข่ายด้วยเซิร์ฟเวอร์ DHCP (โดยปกติจะเป็นเราเตอร์เครือข่าย) บริดจ์จะได้รับ IP แอดเดรสจากเซิร์ฟเวอร์ DHCP หากไม่มีเซิร์ฟเวอร์ DHCP DHCP บริดจ์จะใช้ IP แอดเดรสดีฟอลต์แบบสแตติก **169.254.1.250**

หากคุณต้องการให้บริดจ์ใช้IP แอดเดรสแบบสแตติก ให้ทำตามขั้นตอนต่อไปนี้

1. เข้าใช้ยูทิลิตีบนเบราว์เซอร์ของบริดจ์
2. คลิกแท็บ **Network Setup** (การตั้งค่าเครือข่าย)
3. จากเมนูดรอปดาวน์ *Network Connection Type* (ประเภทการเชื่อมต่อเครือข่าย) ให้เลือก **Static IP**(IP แบบสแตติก)
4. เติมฟิลด์ *Static IP Address* (IP แอดเดรสแบบสแตติก), *Subnet Mask* (ซับเน็ตมาส์ก) และ *Default Gateway* (เกตเวย์ที่เป็นดีฟอลต์)
5. คลิก **Save Settings** (บันทึกการตั้งค่า)

คอมพิวเตอร์หรืออุปกรณ์เชื่อมต่อ Ethernet ผ่านสายใดๆ ที่เปิดใช้บริดจ์ไม่สื่อสารกับอุปกรณ์ไร้สายอื่นๆ (เช่น คอมพิวเตอร์ หรือเครื่องพิมพ์)

ตรวจสอบรายการต่อไปนี้

- ตรวจสอบให้แน่ใจว่าอุปกรณ์ไร้สายอยู่บนเครือข่ายไร้สายเดียวกับคอมพิวเตอร์หรืออุปกรณ์เชื่อมต่อ Ethernet ที่เชื่อมต่อกับบริดจ์
- ตรวจสอบให้แน่ใจว่าใช้ชื่อเครือข่ายไร้สาย (SSID) กับทุกอุปกรณ์บนเครือข่ายไร้สาย
- ตรวจสอบให้แน่ใจว่าอุปกรณ์ทั้งหมดอยู่บนเครือข่าย IP เดียวกัน ใช้ IP แอดเดรสได้

ยูทิลิตีบนเบราว์เซอร์ไม่ยอมรับรหัสผ่านของคุณ

ตรวจสอบรายการต่อไปนี้

- รหัสผ่านตรงตามตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ ตรวจสอบให้แน่ใจว่ารหัสผ่านใช้ตัวพิมพ์ถูกต้องเมื่อป้อนรหัสผ่าน
- หากคุณลืมรหัสผ่านของคุณ คุรสามารถรีเซตบริดจ์ให้เป็นค่าดีฟอลต์จากโรงงาน

 กดปุ่ม **Reset** (รีเซต) ของบริดจ์ค้างไว้ประมาณ 5 นาที รหัสผ่านจะถูกรีเซตให้เป็นค่าดีฟอลต์จากโรงงานคือ **admin** การตั้งค่าบริดจ์อื่นๆจะถูกรีเซตเป็นค่าดีฟอลต์จากโรงงานเช่นกัน (หากต้องการเข้าใช้ยูทิลิตีบนเบราว์เซอร์ ให้ป้อน **admin** ในฟิลด์ *Password* (รหัสผ่าน))

หลังจากคุณสร้างความเปลี่ยนแปลงผ่านยูทิลิตีบนเบราว์เซอร์ การตั้งค่าใหม่ไม่แสดงบนหน้าจอ

บนเว็บเบราเซอร์ของคุณ ให้คลิก **Refresh**(รีเฟรช) หากการตั้งค่าใหม่ยังไม่แสดง โปรดทำตามขั้นตอนต่อไปนี้

1. ถอดสายอะแดปเตอร์ออกจากบริดจ์
2. รอ 5 วินาที แล้วเสียบอะแดปเตอร์กลับเข้ากับบริดจ์
3. บนเว็บเบราเซอร์ของคุณ ให้คลิก **Refresh**(รีเฟรช)

> **เว็บ**
> หากคุณไม่พบคำตอบที่อธิบายข้อสงสัยของคุณในนี้ โปรดดูที่เว็บไซต์ของ Linksys ที่ **Linksys.com/support**

คุณสมบัติเฉพาะ

WES610N

รุ่น	WES610N
มาตรฐาน	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
ไฟ LED	การเปิดปิด, Ethernet, Wi-Fi Protected Setup™, ระบบไร้สาย, การใช้งานและลิงค์ Ethernet แต่ละอัน
พอร์ต	Ethernet (4), การเปิดปิด
ปุ่ม	รีเซ็ต, Wi-Fi Protected Setup
ชนิดของสายเคเบิล	CAT5e
เสาอากาศ	3 (ภายใน)
ชนิดของสายต่อเสาอากาศ	N/A
การถอดออก (ได้/ไม่ได้)	ไม่ได้
การแปลงสัญญาณ	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
การปรับกำลังส่ง (กำลังส่งออกที่มีผล) ในหน่วย dBm	802.11a: 15 dBm (typical) @ 54Mbps 802.11b: 19 dBm (typical) @ 11 Mbps 802.11g: 16 dBm (typical) @ 54 Mbps 802.11n (2.4 GHz): 18 dBm (typical) @ MCS15 802.11n (5 GHz): 16 dBm (typical) @ MCS15
ความแรงสัญญาณ	802.11a: -72 dBm (typical) @ 54 Mbps 802.11b: -85 dBm (typical) @ 11 Mbps 802.11g: -73 dBm (typical) @ 54 Mbps 802.11n (20 MHz): -75 dBm (typical) @ MCS15 802.11n (40 MHz): -69 dBm (typical) @ MCS15
อัตราขยายของเสาอากาศ ในหน่วย dBi	1
การป้องกันไร้สาย	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
จำนวนบิตของคีย์การรักษาความปลอดภัย	เข้ารหัสข้อมูลที่ระดับสูงถึง 128 บิต

คุณสมบัติภายนอก

ขนาดเครื่อง	6.97” x 5.04” x 2.68” (177 x 128 x 68 มม.)
น้ำหนัก	0.65 ปอนด์ (295 กรัม)
การรับรองมาตรฐาน	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
แรงดันไฟฟ้า	12V, 1A
อุณหภูมิในการใช้งาน	32 - 104ºF (0 - 40ºC)
อุณหภูมิในการจัดเก็บ	-4 - 140ºF (-20 - 60ºC)
ความชื้นที่เหมาะสมในการใช้งาน	10 - 85% ไม่มีการควบแน่นของไอน้ำ
ความชื้นที่เหมาะสมในการจัดเก็บ	5 - 90% ไม่มีการควบแน่นของไอน้ำ

คุณสมบัติเฉพาะอาจเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

WET610N

รุ่น	WES610N
มาตรฐาน	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
ไฟ LED	การเปิดปิด, Ethernet, Wi-Fi Protected Setup™, ระบบไร้สาย
พอร์ต	Ethernet (4), การเปิดปิด
ปุ่ม	รีเซ็ต, Wi-Fi Protected Setup
ชนิดของสายเคเบิล	CAT5e
เสาอากาศ	3 (ภายใน)
ชนิดของสายต่อเสาอากาศ	N/A
การถอดออก (ได้/ไม่ได้)	ไม่ได้
การแปลงสัญญาณ	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
การปรับกำลังส่ง (กำลังส่งออกที่มีผล) ในหน่วย dBm	802.11a: 15 dBm (typical) @ 54Mbps 802.11b: 18 dBm (typical) @ 11 Mbps 802.11g: 16 dBm (typical) @ 54 Mbps 802.11n: 12 dBm (typical) @ 130 Mbps (HT20), 270 Mbps (HT40)
ความแรงสัญญาณ	802.11a: -72 dBm (typical) @ 54 Mbps 802.11b: -85 dBm (typical) @ 11 Mbps 802.11g: -73 dBm (typical) @ 54 Mbps 802.11n: -70 dBm (typical) @ MCS15/2.4 GHz, -69 dBm (typical) @ MCS15/5.0 GHz
อัตราขยายของเสาอากาศ ในหน่วย dBi	1
การรักษาความปลอดภัยไร้สาย	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
จำนวนบิตของคีย์การรักษาความปลอดภัย	เข้ารหัสข้อมูลที่ระดับสูงถึง 128 บิต

คุณสมบัติภายนอก

ขนาดเครื่อง	5.71” x 4.17” x 2.05” (145 x 106 x 52 มม.)
น้ำหนัก	5.61 oz (159 g)
การรับรองมาตรฐาน	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
แรงดันไฟฟ้า	12V, 1A
อุณหภูมิในการใช้งาน	32 - 104ºF (0 - 40ºC)
อุณหภูมิในการจัดเก็บ	-4 - 140°F (-20 - 60°C)
ความชื้นที่เหมาะสมในการใช้งาน	10 - 85% ไม่มีการควบแน่นของไอน้ำ
ความชื้นที่เหมาะสมในการจัดเก็บ	5 - 90% ไม่มีการควบแน่นของไอน้ำ

คุณสมบัติเฉพาะอาจเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

Linksys.com/support

Cisco, โลโก้ของ Cisco และ Linksys เป็นเครื่องหมายการค้าหรือเครื่องหมายการค้าจดทะเบียนของ Cisco และ/หรือบริษัทในเครือในประเทศสหรัฐอเมริกา และประเทศอื่นๆ
คุณสามารถดูรายการเครื่องหมายการค้าของ Cisco ได้ที่ www.cisco.com/go/trademarks เครื่องหมายการค้าอื่นๆ ที่อ้างถึงในเอกสารนี้เป็นทรัพย์สินของเจ้าของแต่ละราย

© 2011 Cisco และ/หรือบริษัทในเครือ สงวนลิขสิทธิ์
3425-01249



Kullanıcı Kılavuzu

Linksys WET610N/WES610N | Dual-Band N Entertainment Bridge

İçindekiler

Ürüne Genel Bakış

LED paneli 2
Port paneli 3

Kablosuz Güvenlik Kontrol Listesi

Varsayılan kablosuz ağ adını veya SSID'yi değiştirin 4
Varsayılan parolayı değiştirin 4
MAC adresi filtrelemeyi etkinleştirin 4
Şifrelemeyi etkinleştirin 4

Genel Ağ Güvenlik Kuralları 4
İlave Güvenlik İpuçları 5

Gelişmiş Yapılandırma

Tarayıcı tabanlı yardımcı programa erişim 6
Setup (Ayarlar) > Basic Setup (Temel Ayarlar) 7
Language (Dil) 7
Network Setup (Ağ Ayarları) 7
Wireless (Kablosuz) > Basic Wireless Settings (Temel Kablosuz Ayarları) 7
Basic Wireless Settings (Temel Kablosuz Ayarları) 8
Wireless Security (Kablosuz Güvenliği) 8
Wi-Fi Protected Setup (Wi-Fi Korumalı Kurulum) 9
Wireless (Kablosuz) > Wireless Network Site Survey (Kablosuz Ağ Yer Araştırması) 10
Wireless Network Site Survey (Kablosuz Ağ Yer Araştırması) 10
Wireless (Kablosuz) > WMM® 11
WMM 12
Wireless (Kablosuz) > Advanced Wireless Settings (Gelişmiş Kablosuz Ayarları) 13
Advanced Wireless (Gelişmiş Kablosuz) 14
Administration (Yönetim) > Management (Yönetim) 14
Management (Yönetim) 15
Administration (Yönetim) > Factory Defaults (Fabrika Varsayılanları) 15
Factory Defaults (Fabrika Varsayılanları) 15
Administration (Yönetim) > Upgrade Firmware (Bellenimi Yükselt) 15
Upgrade Firmware (Bellenimi Yükselt) 16
Status (Durum) > Bridge (Köprü) 16
Bridge Information (Köprü Bilgileri) 16
Local Network (Yerel Ağ) 16
Status (Durum) > Wireless (Kablosuz) 16
Wireless (Kablosuz) 16

Sorun giderme

WES610N/WET610N 17

Spesifikasyonlar

WES610N 18
WET610N 19

Ürüne Genel Bakış

Linksys Linksys Dual-Band N Entertainment Bridge'i tercih ettiğiniz için teşekkür ederiz. Köprü kablolu (Ethernet) aygıtlarınızı kablosuz ağınıza bağlayabilir. Köprü, dual-band Kablosuz-N'yi temel alır; bu nedenle, herhangi bir Kablosuz-N, -G, -A, veya -B router'la ya da erişim noktasıyla uyumludur. İlk yükleme sırasında CD klasöründeki adımları uygulayın. Gelişmiş ayarları yapılandırmak için, tarayıcı tabanlı, kullanışlı yardımcı programı kullanın.

LED paneli



WES610N WET610N

Kablosuz (Mavi) Kablosuz LED'i bir kablosuz bağlantı kurulduğunda yanar. Köprü kablosuz ağ üzerinden aktif olarak veri gönderirken veya alırken LED sürekli yanıp söner.

Wi-Fi Korumalı Kurulum Düğmesi Router'ınız Wi-Fi Korumalı Kurulumu destekliyor ve WPA veya WPA2 güvenliğini kullanıyorsa, köprüye otomatik olarak bağlanmak için Wi-Fi Korumalı Kurulumu kullanabilirsiniz. Wi-Fi Korumalı Kurulumu kullanmak için bkz. "Wireless (Kablosuz) > Basic Wireless Settings (Temel Kablosuz Ayarları)", sayfa 7.

Wi-Fi Korumalı Kurulum LED'i (Mavi/Sarı) Bu LED, Wi-Fi Korumalı Kurulum sırasında iki dakika boyunca mavi renkte yanıp söner. Kablosuz güvenliği sağlandığında mavi renkte yanar. Wi-Fi Korumalı Kurulum işlemi sırasında bir hata oluştuğu takdirde, LED kehribar renkte yanar. Ağ router'ının Wi-Fi Korumalı Kurulumu desteklediğinden emin olun. LED sönene kadar bekleyin ve ardından yeniden deneyin.

Ethernet (Mavi) Ethernet LED'i kablolu bir bağlantı kurulduğunda yanar. Köprü Ethernet portu üzerinden aktif olarak veri gönderirken veya alırken LED sürekli yanıp söner.

Güç (Mavi) Güç LED'i köprü açıldığında yanar.

Port paneli



WES610N WET610N

Ethernet Ethernet portları köprüyü bilgisayara veya başka Ethernet ağ aygıtına bağlar. WES610N'de dört, WET610N'deyse tek port bulunur.

Sıfırla Köprüyü üretici varsayılan ayarlarına sıfırlamanın iki yolu vardır. Reset (Sıfırla) düğmesine basın ve yaklaşık beş saniye basılı tutun veya köprünün tarayıcı tabanlı yardımcı programının Administration (Yönetim) > Factory Defaults (Fabrika Varsayılanları) ekranından varsayılan ayarları geri yükleyin. WES610N'de sıfırlama düğmesi aygıtın altında, WET610N'deyse arka port panelindedir.

Güç Power (Güç) portu, köprüyle birlikte verilen güç adaptörüne bağlar.

Kablosuz Güvenlik Kontrol Listesi

Kablosuz ağların kurulması rahat ve kolaydır, bu nedenle de yüksek hızlı İnternet bulunan evlerde hızlı bir şekilde benimsenmektedir. Kablosuz ağlar radyo dalgalarıyla bilgi göndererek çalıştığı için, klasik kablolu ağlara göre izinsiz girişlere daha açık olabilir. Cep veya telsiz telefonlarınızın sinyalleri gibi kablosuz ağınızın sinyalleri de yakalanabilir. Herhangi birisinin kablosuz ağınıza bağlanmasını fiziksel olarak engelleyemeyeceğiniz için, ağınızı güvenli tutmak için bazı ilave adımlar atmanız gerekir.

Varsayılan kablosuz ağ adını veya SSID'yi değiştirin

Kablosuz aygıtların fabrikada atanan varsayılan bir kablosuz ağ adı veya Hizmet Küme Tanımlayıcısı (Service Set Identifier /SSID) vardır. Bu kablosuz ağınızı adıdır ve en fazla 32 karakter uzunluğunda olabilir. Linksys kablosuz ürünleri varsayılan kablosuz ağ adı olarak **linksys**'i kullanırlar. Bu kablosuz ağ adını, kablosuz ağınızı etrafınızda bulunabilecek diğer kablosuz ağlardan ayırt etmenizi sağlayacak benzersiz bir adla değiştirmeniz gerekir, ancak bunu yaparken (SSK sicil numaranız gibi) kişisel bilgilerinizi kullanmayın çünkü bu bilgiler kablosuz ağınız göz atan herhangi biri tarafından görülebilir.

Varsayılan parolayı değiştirin

Erişim noktaları ve router'lar gibi kablosuz ürünlerin ayarlarını değiştirmek istediğinizde bir parola sorulur. Bu aygıtların fabrikada atanmış varsayılan bir parolası vardır. Linksys'in varsayılan parolası **admin**'dir. Bilgisayar korsanları varsayılan parolaları bilir ve kablosuz aygıtınıza erişmek ve ağ ayarlarınızı değiştirmek için bu parolaları kullanmayı deneyebilirler. Bu tür izinsiz değişikliklerin önüne geçmek için, aygıtın parolasını zor tahmin edilecek şekilde özelleştirin.

MAC adresi filtrelemeyi etkinleştirin

Linksys router'ları Media Access Control (MAC) adresi filtrelemeyi etkinleştirmenize olanak verir. MAC adresi her ağ aygıtına atanan benzeriz bir rakam ve harfler dizisidir. MAC adresi filtreleme etkinleştirildiğinde, kablosuz ağa yalnızca belirtilen MAC adreslerine sahip kablosuz aygıtlar erişebilir. Örneğin, evinizdeki her bilgisayarın MAC adresini belirterek yalnızca bu bilgisayarların kablosuz ağınıza bağlanmasını sağlayabilirsiniz.

Şifrelemeyi etkinleştirin

Şifreleme bir kablosuz ağ üzerinden aktarılan verileri koruyabilir. Wi-Fi Protected Access (WPA/WPA2) ve Wired Equivalent Privacy (WEP) kablosuz iletişim için farklı güvenlik seviyeleri sunarlar.

WPA/WPA2 ile şifrelenen bir ağ WEP ile şifrelenen bir ağdan daha güvenlidir, çünkü WPA/WPA2 dinamik anahtar şifreleme kullanır. Havadaki dalgalardan geçen bilgileri korumak için, ağ donanımınızın desteklediği en yüksek şifreleme seviyesini kullanmanız gerekir.

WEP daha eski bir şifreleme standardıdır ancak WPA'yı desteklemeyen bazı eski aygıtlarda kullanılabilir tek seçenek olabilir.

Genel Ağ Güvenlik Kuralları

Kablosuz ağ güvenliği temelindeki ağ güvenli değilse yararsızdır.

- Ağdaki tüm bilgisayarları parolayla koruyun ve hassas dosyaları ayrı parolalarla koruyun.
- Parolaları düzenli aralıklarla değiştirin.
- Anti-virüs yazılımı ve kişisel güvenlik duvarı yazılımı yükleyin.
- Dosya paylaşımını (eş düzeyde) devreden çıkarın. Bazı uygulamalar dosya paylaşımını sizin izniniz ve/veya bilginiz olmadan açabilir.

İlave Güvenlik İpuçları

- Kablosuz router'ları, erişim noktalarını veya ağ geçitlerini dış duvarlardan ve pencerelerden uzak tutun.
- Kablosuz router'ları, erişim noktalarını veya ağ geçitlerini kullanılmadığı zamanlarda (gece, tatilde) kapalı tutun.
- En az sekiz karakter uzunluğunda güçlü parolalar kullanın. Sözlükte bulunabilecek standart sözcüklerden kaçınarak harf ve rakamları birlikte kullanın.

Gelişmiş Yapılandırma

Köprüyü CD klasöründeki aşağıdaki adımlarla kurduktan sonra, köprü kullanıma hazırdır. Bununla birlikte, gelişmiş ayarlarını değiştirmek istiyorsanız, köprünün tarayıcı tabanlı yardımcı programını kullanın. Bu bölümde yardımcı programın her web sayfası ve her sayfanın temel fonksiyonları anlatılmaktadır. Yardımcı programa köprüyle aynı ağa bağlı bir bilgisayardaki web tarayıcısı aracılığıyla erişebilirsiniz.

Tarayıcı tabanlı yardımcı programda şu ana sekmeler bulunur: Setup (Ayarlar), Wireless (Kablosuz), Administration (Yönetim) ve Status (Durum). Ana sekmelerden birisi tıklandığında ilave sekmeler açılır.

Tarayıcı tabanlı yardımcı programa erişim

Tarayıcı tabanlı yardımcı programa erişmek için web tarayıcısı kullanın.

Köprü ağa bir DHCP sunucusuyla (olağan durumda ağ router'ı) bağlıysa, köprü IP adresini DHCP sunucusundan alır. DHCP sunucusu yoksa, köprü varsayılan **169.254.1.250** statik IP adresini kullanır. (Tarayıcı tabanlı yardımcı programıyla köprüde sürekli bir statik IP adresi ayarladıysanız statik IP adresi yerine bunu kullanın.)

NOT
Köprünün IP adresini bilmiyorsanız, IP adresini router'ınızın DHCP istemci tablosunda bulun. (Router'ınızın belgelerine bakın.)

Köprünün IP adresini bulamıyorsanız köprüyü sıfırlayabilirsiniz; düzeltilmiş bir ataş kullanarak yaklaşık beş saniye köprünün **Reset** (Sıfırla) düğmesine basın. Böylece, köprü varsayılan fabrika ayarlarına sıfırlanır. Köprü, DHCP sunucusundan (genellikle ağ router'ı) bir IP adresi isteyecektir. Bulunan DHCP sunucusu yoksa, köprü varsayılan **169.254.1.250** statik IP adresini, bir DHCP sunucusu bulup dinamik bir IP adresi atanana kadar kullanır.

Köprü bir router'la ilişkilendirilmemiş ve fabrika varsayılanlarını kullanıyorsa, web-tabanlı yardımcı programa erişmek için Ethernet bağlantısı kullanarak köprüyü bir bilgisayara bağlayın. Statik IP adresi ve alt ağ maskesiyle bilgisayarda Ethernet bağlantısını yapılandırmanız gerekir.

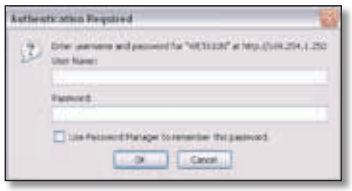
Ethernet adaptörünüzün IP adresi belirli bir IP adresi olarak ayarlanmalıdır.

1. *IP address* (IP adresi) alanına **169.254.x.y** (burada x 1 - 254 arası, y de 0 - 255 arası bir sayı olmalıdır) girin.
2. *Subnet mask* (Alt ağ maskesi) alanına **255.255.0.0** girin.

NOT
Bilgisayarınızdaki Ethernet adaptörüne statik IP adresi atama adımları işletim sistemine göre değişiklik gösterir. Talimatlar için lütfen kendi işletim sisteminizin yardım belgelerine bakın.

Ethernet adaptörünüze statik IP adresi atadıktan sonra web tarayıcınızı başlatıp Adaptörün IP adresini (varsayılan ayar **169.254.1.250**) *Address* (Adres) alanına girin. **Enter** düğmesine basın.

Bir parola istek ekranı görüntülenecektir. (Windows XP olmayan kullanıcılar benzer bir ekran görür.) *User name* (Kullanıcı adı) alanını boş bırakın. Kurulum Sihirbazında oluşturduğunuz parolayı girin. Yeni bir parola oluşturmadıysanız, varsayılan parola olan **admin**'i kullanın. (*Administration* (Yönetim) > *Management* (Yönetim) ekranından yeni bir parola oluşturabilirsiniz.) Devam etmek için **OK** (Tamam) düğmesini tıklatın.



NOT
Parola istek ekranı görüntülenmezse, iki dakika bekleyin ve yeniden deneyin.

Setup (Ayarlar) > Basic Setup (Temel Ayarlar)

Görüntülenen ilk ekran *Basic Setup* (Temel Ayarlar) olacaktır. Tarayıcı tabanlı yardımcı programın dilini değiştirmek veya köprünün kablolu Ethernet ağının ayarlarını değiştirmek için bu ekranı kullanın.





Language (Dil)

Language (Dil) Web tabanlı yardımcı program tarafından görüntülenen dili ayarlamak için kullanılır. Aşağı açılır menüden istediğiniz dili seçin.

Network Setup (Ağ Ayarları)

Bu bölümde, köprünün IP Adresini ağ router'ınız gibi bir DHCP sunucusundan (Otomatik Yapılandırma - DHCP) otomatik olarak mı elde edileceği veya elle mi ayarlanacağı (Statik IP) belirlenir.

Bridge IP (Köprü IP) Ağınızın ağ aygıtlarınıza IP adresleri atayan ağ router'ınız gibi bir DHCP sunucusu varsa, varsayılan ayar olan **Automatic Configuration - DHCP** (Otomatik Yapılandırma - DHCP) ayarını koruyun. Köprü, DHCP sunucusundan (genellikle ağ router'ı) bir IP adresi isteyecektir. Bulunan DHCP sunucusu yoksa, köprü varsayılan **169.254.1.250** statik IP adresini, bir DHCP sunucusu bulup dinamik bir IP adresi atanana kadar kullanır.

Köprü için sürekli bir statik IP adresi atamak istiyorsanız, **Static IP** (Statik IP) ayarını seçin.

Static IP (Statik IP) ayarını seçtiğiniz takdirde, aşağıdaki alanları da doldurun.

- **Static IP Address** (Statik IP Adresi) Tarayıcı tabanlı yardımcı programa erişmek için kullanılacak benzersiz bir IP adresi girin.
- **Subnet Mask** (Alt-ağ Maskesi) Kablolu ağınızın alt-ağ maskesini girin.
- **Default Gateway** (Varsayılan Ağ Geçidi) Ağınızın varsayılan ağ geçidinin (çoğu durumda, router'ınızın) IP adresini girin.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Wireless (Kablosuz) > Basic Wireless Settings (Temel Kablosuz Ayarları)

Köprünün temel kablosuz ve güvenlik ayarlarını yapılandırmak için *Basic Wireless Settings* (Temel Kablosuz Ayarları) ekranını kullanın.

Köprünün ayarlarını değiştirmenin iki yolu vardır: Elle ve Wi-Fi Korumalı Kurulum. Wi-Fi Korumalı Kurulum kablosuz ağınızı kurmanızı kolaylaştıran bir özelliktir. Router'ınız Wi-Fi Korumalı Kurulumu destekliyor ve WPA veya WPA2 güvenliğini kullanıyorsa, köprüye otomatik olarak bağlanmak için Wi-Fi Korumalı Kurulumu kullanabilirsiniz.

Configuration View (Yapılandırma Ekranı) Kablosuz ağınızı elle kurmak için **Manual** (Elle) öğesini seçin. Bkz. "**Basic Wireless Settings** (Temel Kablosuz Ayarları)", **sayfa 8**. Wi-Fi Korumalı Kurulumu kullanmak için, **Wi-Fi Protected Setup** (Wi-Fi Korumalı Kurulum) seçeneğini seçin. Bkz. "**Wi-Fi Protected Setup** (Wi-Fi Korumalı Kurulum)", **sayfa 9**.

Basic Wireless Settings (Temel Kablosuz Ayarları)



Network Name (SSID) (Ağ Adı (SSID)) SSID bir kablosuz ağdaki tüm noktaların ortak ağ adıdır. SSID, kablosuz ağ üzerindeki tüm aygıtlar için aynı olmalıdır. Büyük/küçük harf duyarlıdır ve 32 karakteri aşmamalıdır (klavye üzerindeki her karakter kullanılabilir). Bu ayarın kablosuz router'ınızdaki veya erişim noktanızdaki ayarla eşleştiğinden emin olun. Daha fazla güvenlik için, varsayılan SSID (**linksys**) yerine benzersiz bir ad kullanmanız gerekir.

Wireless Security (Kablosuz Güvenliği)

Köprü, aşağıdaki kablosuz güvenlik seçeneklerini destekler: WPA Kişisel, WPA2 Kişisel ve WEP. WPA (Wi-Fi Protected Access) ve WPA2, WEP (Wired Equivalent Privacy) yöntemine göre daha güçlü güvenlik yöntemleridir. Kablosuz güvenliği hakkında daha fazla bilgi için bkz. "Kablosuz Güvenlik Kontrol Listesi", sayfa 4.

Security Mode (Güvenlik Modu)

Kablosuz ağınız için güvenlik yöntemini seçin. Kablosuz güvenliğini kullanmak istemiyorsanız, varsayılan **Disabled** (Devre dışı) ayarını koruyun.

NOT
Kablosuz ağınızdaki her aygıtın aynı güvenlik yöntemini ve parolasını/anahtarını kullanması gerektiğini, aksi takdirde kablosuz aygıtların birbirleriyle iletişim kuramadığını unutmayın.

WPA Personal (WPA Kişisel)

WPA, WEP şifrelemesine göre daha güçlü bir güvenlik standardıdır.



Encryption (Şifreleme) WPA, dinamik şifreleme anahtarlarıyla TKIP şifreleme yöntemini destekler.

Passphrase (Parola) Köprü ve kablosuz router'ınızın (veya erişim noktanızın) paylaştığı anahtarı girin. 8-63 karakterden oluşmalıdır.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

WPA2 Personal (WPA2 Kişisel)

WPA2, WPA'nin daha gelişmiş ve güvenli bir sürümüdür.



Encryption (Şifreleme) WPA2, dinamik şifreleme anahtarlarıyla iki şifreleme yöntemini destekler: TKIP ve AES. Şifreleme yöntemini **(AES** veya **TKIP veya AES) seçin**. Varsayılan seçim **AES**'tir.

Passphrase (Parola) Köprü ve kablosuz router'ın (veya erişim noktasının) paylaştığı anahtarı girin. 8-63 karakterden oluşmalıdır.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

WEP

WEP, WPA veya WPA2 kadar güvenli olmayan temel bir şifreleme yöntemidir.



Encryption (Şifreleme) Bir WEP şifreleme seviyesi seçin**: 40/64 bits (10 hex digits)** (40 / 64 bit (10 onaltılı basamak)) veya **104/128 bits (26 hex digits)** (104 / 128 bit (26 onaltılı basamak)). Varsayılan ayar **40/64 bits (10 hex digits)** (40 / 64 bit (10 onaltılı basamak)) ayarıdır.

Key 1 (Anahtar 1) Ağınızın anahtarını girin.

Tx Key (Aktarım Anahtarı) **Key 1** (Anahtar 1) köprü tarafından kullanılan aktarım anahtarıdır.

Authentication (Kimlik Doğrulama) Varsayılan **Auto** (Otomatik) ayarı Open (Açık) sistem veya Shared (Paylaşılan) anahtar kimlik doğrulamalarından birisinin kullanılmasını sağlar. Açık sistem kimlik doğrulamasını kullanmak için **Open** (Açık) seçeneğini belirleyin; gönderen ve alan kimlik doğrulama için bir WEP anahtarı kullanmaz. Paylaşılan anahtar kimlik doğrulamasını kullanmak için **Shared** (Paylaşılan) seçeneğini belirleyin; gönderen ve alan kimlik doğrulama için bir WEP anahtarı kullanır.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Wi-Fi Protected Setup (Wi-Fi Korumalı Kurulum)

İki farklı yöntemden biri kullanılabilir. Kullandığınız router'a uygulanan yöntemi kullanın.





Yöntem No 1

Bu yöntemi router'ınızın Wi-Fi Korumalı Kurulum düğmesi varsa kullanın.

1. Router'daki **Wi-Fi Protected Setup** (Wi-Fi Korumalı Kurulum) düğmesine basın veya tıklatın.
2. İki dakika içinde, router'ın *Wi-Fi Protected Setup* (Wi-Fi Korumalı Kurulum) ekranında **Wi-Fi Protected Setup** (Wi-Fi Korumalı Kurulum) düğmesini tıklatın.
3. Router'ınız yapılandırıldıktan sonra, **OK** (Tamam) düğmesini tıklatın.

Wi-Fi Protected Setup (Wi-Fi Korumalı Kurulum) ekranı Link Status (Bağlantı Durumu), Network Name (SSID) (Ağ Adı (SSID)) ve Security (Güvenlik) yöntemini görüntüler.

Yöntem No 2

Router'ınız köprünün PIN numarasını isterse bu yöntemi kullanın.

1. **Router**'ın *Wi-Fi Protected Setup* (Wi-Fi Korumalı Kurulum) ekranına, **köprünün** *Wi-Fi Protected Setup* (Wi-Fi Korumalı Kurulum) ekranındaki PIN numarasını girin. Ardından **Register** (Kaydet) düğmesine veya ilgili düğmeye basın. (Köprünün altındaki etikette de bulunur.)
2. **Köprünün** *Wi-Fi Protected Setup* (Wi-Fi Korumalı Kurulum) ekranında **OK** (Tamam) düğmesini tıklatın.
3. Router'ınız yapılandırıldıktan sonra, **OK** (Tamam) düğmesini tıklatın.

Wi-Fi Protected Setup (Wi-Fi Korumalı Kurulum) ekranı Link Status (Bağlantı Durumu), Network Name (SSID) (Ağ Adı (SSID)) ve Security (Güvenlik) yöntemini görüntüler.

Wireless (Kablosuz) > Wireless Network Site Survey (Kablosuz Ağ Yer Araştırması)

Yer araştırmasını başlatmak için **Wireless Network Site Survey** (Kablosuz Ağ Alan Araştırması) seçeneğini tıklatın. *Wireless Network Site Survey* (Kablosuz Ağ Alan Araştırması) ekranında köprünün algıladığı kablosuz ağların listesi görüntülenir.



Wireless Network Site Survey (Kablosuz Ağ Yer Araştırması)

Number of Wireless Networks (Kablosuz Ağ Sayısı) Köprünün algıladığı kablosuz ağ sayısı görüntülenir.

Select (Seç) Kablosuz ağa bağlanmak için **Select** (Seç) seçeneğini tıklatın. Ardından **Connect** (Bağlan) düğmesini tıklatın.

Wireless Network Name (Kablosuz Ağ Adı) Kablosuz ağın ağ adı veya SSID'si görüntülenir.

GHz Kablosuz ağın radyo bandı görüntülenir.

Signal (Sinyal) Sinyal gücünün yüzde değeri görüntülenir. %100 olası en güçlü sinyaldir; %0 da olası en zayıf olanıdır.

Security (Güvenlik) Ağ Wi-Fi Korumalı Kurulumu destekliyorsa, Wi-Fi Korumalı Kurulum simgesi görüntülenir. Kablosuz ağınız tarafından kullanılan güvenlik yöntemi görüntülenir.

Ekrandaki verileri güncellemek için **Refresh** (Yenile) düğmesini tıklatın.

Ağı seçtikten sonra **Connect** (Bağlan) düğmesini tıklatın. Yeni bir ekran görüntülenir. Ağınızın güvenlik yöntemi için talimatları uygulayın.

WPA



Network Name (SSID) (Ağ Adı (SSID)) Seçtiğiniz ağ adı otomatik olarak görüntülenir.

Security Mode (Güvenlik Modu) WPA Personal otomatik olarak görüntülenir.

Encryption (Şifreleme) WPA, dinamik şifreleme anahtarlarıyla TKIP şifreleme yöntemini destekler.

Passphrase (Parola) Köprü ve kablosuz router'ın (veya erişim noktasının) paylaştığı anahtarı girin. 8-63 karakterden oluşmalıdır.

Ekrandaki verileri güncellemek için **Refresh** (Yenile) düğmesini tıklatın.

Güvenlik ayarlarını girdikten sonra **Connect** (Bağlan) düğmesini tıklatın.

WPA2



Network Name (SSID) (Ağ Adı (SSID)) Seçtiğiniz ağ adı otomatik olarak görüntülenir.

Security Mode (Güvenlik Modu) WPA2 Personal otomatik olarak görüntülenir.

Encryption (Şifreleme) WPA2, dinamik şifreleme anahtarlarıyla iki şifreleme yöntemini destekler: TKIP ve AES. Şifreleme yöntemini **(AES** veya **TKIP veya AES) seçin**.

Passphrase (Parola) Köprü ve kablosuz router'ın (veya erişim noktasının) paylaştığı anahtarı girin. 8-63 karakterden oluşmalıdır.

Ekrandaki verileri güncellemek için **Refresh** (Yenile) düğmesini tıklatın.

Güvenlik ayarlarını girdikten sonra **Connect** (Bağlan) düğmesini tıklatın.

WEP



Network Name (**SSID** - Ağ Adı) Seçtiğiniz ağ adı otomatik olarak görüntülenir.

Security Mode (Güvenlik Modu) WEP otomatik olarak görüntülenir.

Encryption (Şifreleme) Bir WEP şifreleme seviyesi seçin: **40/64 bits (10 hex digits)** veya **104/128 bits (26 hex digits)**.

Key 1 (Anahtar 1) Ağınızın anahtarını girin.

Tx Key (Aktarım Anahtarı) **Key 1** (Anahtar 1) köprü tarafından kullanılan aktarım anahtarıdır.

Authentication (Kimlik Doğrulama) Varsayılan **Auto** (Otomatik) ayarı Open (Açık) sistem veya Shared (Paylaşılan) anahtar kimlik doğrulamalarından birisinin kullanılmasını sağlar. Açık sistem kimlik doğrulamasını kullanmak için **Open** (Açık) seçeneğini belirleyin; gönderen ve alan kimlik doğrulama için bir WEP anahtarı kullanmaz. Paylaşılan anahtar kimlik doğrulamasını kullanmak için **Shared** (Paylaşılan) seçeneğini belirleyin; gönderen ve alan kimlik doğrulama için bir WEP anahtarı kullanır.

Ekrandaki verileri güncellemek için **Refresh** (Yenile) düğmesini tıklatın.

Güvenlik ayarlarını girdikten sonra **Connect** (Bağlan) düğmesini tıklatın.

Wireless (Kablosuz) > WMM®

Wireless MultiMedia (WMM) [Kablosuz Multimedya] ayarlarını yapılandırın. WMM, kendi erişim moduna (trafik tipi) göre paketlere öncelik verir: Background (Arka Plan), Best Effort (En Yüksek Gayret), Video veya Voice (Ses). Bu ayarlar, hatalı ayarlar kablosuz performansını azaltabileceği için, yalnızca uzman bir yönetici tarafından yapılmalıdır.



NOT
WMM ekranındaki ayarlar yalnızca gelişmiş kullanıcılar için tasarlanmıştır.

WMM

Access Mode (Erişim Modu)

Kullanılabilir dört erişim moduna farklı ayarlar atayabilirsiniz. Yapılandırmak istediğiniz modu seçin. **Background** (Arka Plan), **Best Effort** (En Yüksek Gayret), **Video** veya **Voice** (Ses). Seçtiğiniz modun yönergelerini uygulayın.

Background (Arka Plan)

Use Aggregation (Biriktirme Kullan) Bu seçenek Media Access Control (MAC) katmanının bir Add Block Acknowledgement (ADDBA) oturumu oluşturup oluşturmayacağını tanımlar. **No** (Hayır) varsayılan öğedir. Bu seçeneği etkinleştirmek için **Yes** (Evet) öğesini seçin.

Accept Aggregation (Biriktirme Kabul Et) Bu seçenek MAC katmanının bir ADDBA isteğini kabul edip etmeyeceğini tanımlar. Varsayılan ayar: **Yes** (Evet). Bu seçeneği devreden çıkarmak için **No** (Hayır) ayarını seçin.

Max. Number of Packets in Aggregation (Maks. Biriktirme Paket Sayısı) Bu seçenek biriktirilen maksimum paket (alt çerçeve) sayısını tanımlar. Geçerli aralık: **0** - **7**. Varsayılan ayar **7**'dir.

Max. Aggregation Size (Maks. Biriktirme Boyutu) Bu seçenek maksimum biriktirme boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **16000**. Varsayılan ayar **12000**'dir.

Timeout Internal (İç Zamanaşımı) Bu seçenek, biriktirme işleminin bitiminde zamanlayıcı tarafından bir "kapatma koşuluyla" kapatılması gereken zamanaşımı süresini tanımlar. Geçerli aralık: **0** - **100**. Varsayılan ayar **3**'tür.

Min. Size of Packet in Aggregation (Min. Paket Biriktirme Boyutu) Bu seçenek biriktirilecek minimum paket boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **1500**. Varsayılan ayar **10**'dur.

ADDBA Timeout (ADDBA Zamanaşımı) Bu seçenek, çerçeve alışverişinin olmadığı hangi sürenin sonunda ADDBA ayarının Block Acknowledgement (ACK) anlaşması tarafından sona erdirileceğini tanımlar. Geçerli aralık: **0** - **65535**. Varsayılan ayar, zamanaşımını devreden çıkaran **0**'dır.

Aggregation Window Size (Biriktirilmiş Pencere Boyutu) Bu seçenek, ACK alınmadan aktarılan maksimum paket sayısını tanımlar. Geçerli aralık: **0** - **64**. Varsayılan ayar **64**'tür.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Best Effort (En Yüksek Gayret)

Use Aggregation (Biriktirme Kullan) Bu seçenek Media Access Control (MAC) katmanının bir Add Block Acknowledgement (ADDBA) oturumu oluşturup oluşturmayacağını tanımlar. Varsayılan ayar: **Yes** (Evet). Bu seçeneği devreden çıkarmak için **No** (Hayır) ayarını seçin.

Accept Aggregation (Biriktirme Kabul Et:) Bu seçenek MAC katmanının bir ADDBA isteğini kabul edip etmeyeceğini tanımlar. Varsayılan ayar: **Yes** (Evet). Bu seçeneği devreden çıkarmak için **No** (Hayır) ayarını seçin.

Max. Number of Packets in Aggregation (Maks. Biriktirme Paket Sayısı) Bu seçenek biriktirilen maksimum paket (alt çerçeve) sayısını tanımlar. Geçerli aralık: **0** - **10**. Varsayılan ayar **10**'dur.

Max. Aggregation Size (Maks. Biriktirme Boyutu) Bu seçenek maksimum biriktirme boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **20000**. Varsayılan ayar **16000**'dir.

Timeout Internal (İç Zamanaşımı) Bu seçenek, biriktirme işleminin bitiminde zamanlayıcı tarafından bir "kapatma koşuluyla" kapatılması gereken zamanaşımı süresini tanımlar. Geçerli aralık: **0** - **100**. Varsayılan ayar **3**'tür.

Min. Size of Packet in Aggregation (Min. Paket Biriktirme Boyutu) Bu seçenek biriktirilecek minimum paket boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **1500**. Varsayılan ayar **10**'dur.

ADDBA Timeout (ADDBA Zamanaşımı) Bu seçenek, çerçeve alışverişinin olmadığı hangi sürenin sonunda ADDBA ayarının Block Acknowledgement (ACK) anlaşması tarafından sona erdirileceğini tanımlar. Geçerli aralık: **0** - **65535**. Varsayılan ayar, zamanaşımını devreden çıkaran **0**'dır.

Aggregation Window Size (Biriktirilmiş Pencere Boyutu) Bu seçenek, ACK alınmadan aktarılan maksimum paket sayısını tanımlar. Geçerli aralık: **0** - **64**. Varsayılan ayar **64**'tür.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Video (Video)

Use Aggregation (Biriktirme Kullan) Bu seçenek Media Access Control (MAC) katmanının bir Add Block Acknowledgement (ADDBA) oturumu oluşturup oluşturmayacağını tanımlar. Varsayılan ayar: **Yes** (Evet). Bu seçeneği devreden çıkarmak için **No** (Hayır) ayarını seçin.

Accept Aggregation (Biriktirme Kabul Et) Bu seçenek MAC katmanının bir ADDBA isteğini kabul edip etmeyeceğini tanımlar. Varsayılan ayar: **Yes** (Evet). Bu seçeneği devreden çıkarmak için **No** (Hayır) ayarını seçin.

Max. Number of Packets in Aggregation (Maks. Biriktirme Paket Sayısı) Bu seçenek biriktirilen maksimum paket (alt çerçeve) sayısını tanımlar. Geçerli aralık: **0** - **7**. Varsayılan ayar **7**'dir.

Max. Aggregation Size (Maks. Biriktirme Boyutu) Bu seçenek maksimum biriktirme boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **16000**. Varsayılan ayar **12000**'dir.

Timeout Internal (İç Zamanaşımı) Bu seçenek, biriktirme işleminin bitiminde zamanlayıcı tarafından bir "kapatma koşuluyla" kapatılması gereken zamanaşımı süresini tanımlar. Geçerli aralık: **0** - **100**. Varsayılan ayar **3**'tür.

Min. Size of Packet in Aggregation (Min. Paket Biriktirme Boyutu) Bu seçenek biriktirilecek minimum paket boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **1500**. Varsayılan ayar **10**'dur.

ADDBA Timeout (ADDBA Zamanaşımı) Bu seçenek, çerçeve alışverişinin olmadığı hangi sürenin sonunda ADDBA ayarının Block Acknowledgement (ACK) anlaşması tarafından sona erdirileceğini tanımlar. Geçerli aralık: **0** - **65535**. Varsayılan ayar, zamanaşımını devreden çıkaran **0**'dır.

Aggregation Window Size (Biriktirilmiş Pencere Boyutu) Bu seçenek, ACK alınmadan aktarılan maksimum paket sayısını tanımlar. Geçerli aralık: **0** - **64**. Varsayılan ayar **64**'tür.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Voice (Ses)

Use Aggregation (Biriktirme Kullan) Bu seçenek Media Access Control (MAC) katmanının bir Add Block Acknowledgement (ADDBA) oturumu oluşturup oluşturmayacağını tanımlar. Varsayılan ayar: **Yes** (Evet). Bu seçeneği devreden çıkarmak için **No** (Hayır) ayarını seçin.

Accept Aggregation (Biriktirme Kabul Et) Bu seçenek MAC katmanının bir ADDBA isteğini kabul edip etmeyeceğini tanımlar. Varsayılan ayar: **Yes** (Evet). Bu seçeneği devreden çıkarmak için **No** (Hayır) ayarını seçin.

Max. Number of Packets in Aggregation (Maks. Biriktirme Paket Sayısı) Bu seçenek biriktirilen maksimum paket (alt çerçeve) sayısını tanımlar. Geçerli aralık: **0** - **2**. Varsayılan ayar **2**'dir.

Max. Aggregation Size (Maks. Biriktirme Boyutu) Bu seçenek maksimum biriktirme boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **16000**. Varsayılan ayar **10000**'dir.

Timeout Internal (İç Zamanaşımı) Bu seçenek, biriktirme işleminin bitiminde zamanlayıcı tarafından bir "kapatma koşuluyla" kapatılması gereken zamanaşımı süresini tanımlar. Geçerli aralık: **0** - **100**. Varsayılan ayar **10**'dur.

Min. Size of Packet in Aggregation (Min. Paket Biriktirme Boyutu) Bu seçenek biriktirilecek minimum paket boyutunu (bayt olarak) tanımlar. Geçerli aralık: **0** - **1500**. Varsayılan ayar **10**'dur.

ADDBA Timeout (ADDBA Zamanaşımı) Bu seçenek, çerçeve alışverişinin olmadığı hangi sürenin sonunda ADDBA ayarının Block Acknowledgement (ACK) anlaşması tarafından sona erdirileceğini tanımlar. Geçerli aralık: **0** - **65535**. Varsayılan ayar, zamanaşımını devreden çıkaran **0**'dır.

Aggregation Window Size (Biriktirilmiş Pencere Boyutu) Bu seçenek, ACK alınmadan aktarılan maksimum paket sayısını tanımlar. Geçerli aralık: **0** - **64**. Varsayılan ayar **64**'tür.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Wireless (Kablosuz) > Advanced Wireless Settings (Gelişmiş Kablosuz Ayarları)

Köprünün gelişmiş kablosuz fonksiyonlarını yapılandırın. Bu ayarlar, hatalı ayarlar kablosuz performansını azaltabileceği için, yalnızca uzman bir yönetici tarafından yapılmalıdır.



NOT
Advanced Wireless Settings (Gelişmiş Kablosuz Ayarları) ekranındaki ayarlar yalnızca gelişmiş kullanıcılar içindir.

Advanced Wireless (Gelişmiş Kablosuz)

Use LDPC (LDPC Kullan) Düşük Yoğunluklu Parite Kontrol Kodu (LDPC), gürültülü kanallarda veri kaybı olasılığını azaltmak için hata düzeltmeyi etkinleştirir veya devre dışı bırakır. Rate Adaptation (Hız Uyarlaması) algoritması, yüksek PHY hızlarında (162 üstü) çalışıldığında LDPC kodlamasını otomatik olarak devre dışı bırakır. LDCP gelişmiş hata düzeltme düzenini kullanmak için varsayılan **Yes** (Evet) değerini koruyun. İstemiyorsanız, **No** (Hayır) seçeneğini belirleyin.

ERP Protection Type (ERP Koruma Türü) Bu seçenek, kablosuz ağdaki 802.11b istasyonlarının varlığı yerine OFDM paketlerinin korunmasını yapılandırır. RTS/CTS veya CTS2Self paketlerini 802.11b hızlarında göndererek, köprü kablosuz ağa OFDM paketlerinin aktarılmak üzere olduğunu ve kablosuz ağdaki paketleri koruduğunu bildirir. RTS/CTS ve CTS2Self paketleri düşük akışa neden olabilecek tepeyi oluşturur.

RTS/CTS seçeneği, CTS2Self ile karşılaştırıldığında daha iyi kapsam sağlasa da daha düşük akışa sahiptir; RTS/CTS seçeneğinde alacı aygıta ait bildirim buna neden olur. RTS/CTS seçeneğini kullanmak için varsayılan **RTS/CTS** seçeneğini koruyun. None (Hiçbiri) seçeneği OFDM ve CCK paketleri arasında çakışmalara neden olabilir. None (Hiçbiri) seçeneğini kullanmak için **None** (Hiçbiri) seçeneğini belirleyin. CTS2Self seçeneğini kullanmak için **CTS2Self** seçeneğini belirleyin.

11n Protection Type (11n Koruma Türü) Bu seçenek, kasblosuz ağdaki non-High Throughput (HT) aygıtlara ait korumayı yapılandırır. Kablosuz router'ın (veya erişim noktasının) non-HT eski aygıtıyla ilişkilendirilmesini saptadığı durumda, her veri iletiminden önce tüm HT aygıtlarının RTS/CTS veya CTS2Self mekanizmalarını kullanma sinyalini gönderir. Bu özellik, MIMO dahil, tüm 802.11n standart korumalarını da destekler.

RTS/CTS seçeneği, CTS2Self ile karşılaştırıldığında daha iyi kapsam sağlasa da daha düşük akışa sahiptir; RTS/CTS seçeneğinde alacı aygıta ait bildirim buna neden olur. RTS/CTS seçeneğini kullanmak için varsayılan **RTS/CTS** seçeneğini koruyun. None (Hiçbiri) seçeneği HT ve eski paketler arasında çakışmalara neden olabilir. None (Hiçbiri) seçeneğini kullanmak için **None** (Hiçbiri) seçeneğini belirleyin. CTS2Self seçeneğini kullanmak için **CTS2Self** seçeneğini belirleyin.

Percentage of maximal transmit power (Maksimum Aktarım Gücü Yüzdesi) Bu seçenek düzenleyici alan sınırlamalarıyla bağlantılı maksimum aktarım gücü yüzdesini ayarlar. Örneğin, düzenleyici alan sınırlaması 20 dB'a kadar aktarımlara izin veriyorsa, 50% ayarı 10 dB maksimum aktarım gücüne izin verir. Kullanmak istediğiniz yüzdeyi seçin. **%12**, **%25**, **%50** veya **%100**. Varsayılan ayar: **100%**

QoS Classification Type (QoS Sınıflandırma Türü) Bu seçenek 802.1D veya 802.1Q eşlemeyi IP DSCP/TOS alanından WMM öncelikleri (Background (Arka Plan), Best Effects (En Yüksek Gayret), Video, Voice (Ses)) olarak ayarlar. Varsayılan **802.1D** değerini ya da bazı IPTV akışlarının kullandığı **802.1Q** değerini koruyun.

Re-establish Ethernet connection when initiating wireless connection (Kablosuz bağlantı başlatıldığında Ethernet bağlantısını yeniden başlat) Köprünün ardında kalan aygıttan DHCP algılamayı tetiklemek için, kablosuz bağlantı her başlatıldığında, köprü aygıtla arasındaki Ethernet bağlantısını sıfırlar. Bu davranışı devre dışı bırakmak için **No** (Hayır) seçeneğini belirleyin. Varsayılanı korumak için de **Yes** (Evet) seçeneğini belirleyin.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Administration (Yönetim) > Management (Yönetim)

Bu ekranı belirli köprü işlevlerini yönetmek için kullanın: web-tabanlı yardımcı programa erişme, yapılandırma dosyasını yedekleme ve yeniden başlatma.



Management (Yönetim)

Köprü Erişimi

Tarayıcı tabanlı yardımcı programa erişimi korumak için parola kullanın.

Bridge Password (Köprü Parolası) Köprü için yeni bir parola girin.

Re-enter to confirm (Onaylamak için yeniden girin) Onaylamak için Parolayı yeniden girin.

Idle Timeout (Boşta Zamanaşımı) Belirttiğiniz bir işlemsizlik süresinden sonra oturum zamanaşımı. Geçerli aralık: **60** - **3600** saniye. Varsayılan ayar **600**'dür.

Web Access (Web Erişimi)

Access via Wireless (Kablosuz Erişim) Köprüyü konuklarınıza kablosuz erişim yetkisi verdiğiniz halka açık bir etki alanında kullanıyorsanız, köprünün tarayıcı tabanlı yardımcı programına kablosuz erişimi devreden çıkarabilirsiniz. Ayarı devreden çıkardığınız takdirde, tarayıcı tabanlı yardımcı programa yalnızca bir kablolu bağlantıyla erişebilirsiniz. Köprünün yardımcı programına kablosuz erişime izin vermek için varsayılan **Enabled** (Etkin) ayarını koruyun veya yardımcı programa kablosuz erişimi engellemek için **Disabled** (Devre dışı) ayarını seçin.

Backup (Yedekle) ve Restore (Geri Yükle)

Backup (Yedekle) Köprünün yapılandırma dosyasını yedeklemek için, **Backup Configurations** (Yapılandırmaları Geri Yükle) düğmesini tıklatın. Ardından ekrandaki yönergeleri izleyin.

Restore (Geri Yükle) **Browse** (Gözat) düğmesini tıklatıp yapılandırma dosyasını seçin. Ardından **Restore Configurations** (Yapılandırmaları Geri Yükle) düğmesini tıklatın.

System Reboot (Sistemi Yeniden Başlat)

Reboot (Yeniden Başlat) Köprüyü yeniden Başlatmak için, **Start to Reboot** (Yeniden Başlat) düğmesini tıklatın.

Değişikliklerinizi uygulamak için **Save Settings** (Ayarları Kaydet) düğmesini veya değişikliklerinizi iptal etmek için **Cancel Changes** (Değişiklikleri İptal Et) düğmesini tıklatın.

Administration (Yönetim) > Factory Defaults (Fabrika Varsayılanları)

Bu ekranı köprünün yapılandırmasını fabrika varsayılan ayarlarına geri döndürmek için kullanın.

Factory Defaults (Fabrika Varsayılanları)

Restore All Settings (Tüm Ayarları Geri Yükle) Köprünün ayarlarını fabrika ayarlarına geri döndürmek için, **Restore All Settings** (Tüm Ayarları Geri Yükle) düğmesini tıklatın. Varsayılan değerler geri yüklendiğinde kaydettiğiniz tüm ayarlarınız kaybolur.



Administration (Yönetim) > Upgrade Firmware (Bellenimi Yükselt)

Köprünün bellenimini yükseltmek için bu ekranı kullanın. Bellenimi köprüde sorun veya yeni bellenimde kullanmak istediğiniz bir özellik yoksa yükseltmeyin.



Köprü bellenimini yükseltmeden önce, Linksys web sitesinden (**www.linksys.com/support**) ürün bilgisi yükseltme yazılımını yükleyin.

Upgrade Firmware (Bellenimi Yükselt)

Lütfen bellenimi yükseltmek için bir dosya seçin **Browse** (Gözat) düğmesini tıklatın ve bellenim yükseltme dosyasını seçin. Ardından **Start to Upgrade** (Yükseltmeye Başla) düğmesini tıklatın ve ekrandaki yönergeleri uygulayın.

Status (Durum) > Bridge (Köprü)

Köprünün geçerli durumu görüntülenir.



Bridge Information (Köprü Bilgileri)

Firmware Version (Bellenim Sürümü) Köprünün geçerli bellenimi görüntülenir.

Local Network (Yerel Ağ)

Local MAC Address (Yerel MAC Adresi) Köprünün MAC Adresi, yerel Ethernet ağınızda görülen şekilde gösterilir.

IP Address (IP Adresi) Köprünün IP adresini yerel Ethernet ağınızda görüldüğü şekilde görüntüler.

Subnet Mask (Alt-Ağ Maskesi) Yerel ağınız için yapılandırılan Alt-Ağ Maskesi görüntülenir.

Status (Durum) > Wireless (Kablosuz)

Kablosuz ağınız ile ilgili bilgiler görüntülenir.



Wireless (Kablosuz)

Link Status (Bağlantı Durumu) Kablosuz ağınızdaki bağlantının durumu görüntülenir.

MAC Address (MAC Adresi) Köprünün MAC Adresi, yerel kablosuz ağınızda görülen şekilde gösterilir.

Network Name (SSID) (Ağ Adı (SSID)) Kablosuz ağ adı veya SSID gösterilir.

BSSID Bağlı kablosuz router'ın (veya erişim noktasının) kablosuz MAC adresi görüntülenir.

Radio Band (Radyo Bandı) Kablosuz ağınızın radyo bandı görüntülenir.

Channel Width (Kanal Genişliği) kablosuz ağınızın kullandığı, MHz cinsinden kanal genişliği görüntülenir.

Wide Channel (Geniş Kanal) Ağ router'ınızın kanal ayarlarına bağlı olarak, Geniş Kanal gösterilir. Router'ın Radio Band (Radyo Bandı) veya Channel Width (Kanal Genişliği) olarak Wide - 40MHz Channel (Geniş - 40MHz Kanal) seçtiyseniz, bu birincil Kablosuz-N kanalınız olacaktır.

Standard Channel (Standart Kanal) Standart Kanal ayarı görüntülenir. Router'ın Radio Band (Radyo Bandı) veya Channel Width (Kanal Genişliği) olarak Wide - 40MHz Channel (Geniş - 40MHz Kanal) seçtiyseniz, Standard Channel (Standart Kanal) ikincil Kablosuz-N kanalınız olacaktır.

Bit Rate (Bit Hızı) Veri iletimi hızı görüntülenir.

Signal (Sinyal) Sinyal gücünün yüzde değeri görüntülenir. %100 olası en güçlü sinyaldir; %0 da olası en zayıf olanıdır.

Security (Güvenlik) Kablosuz ağınız tarafından kullanılan güvenlik yöntemi görüntülenir.

Sorun giderme

WES610N/WET610N

Bilgisayarınız veya diğer kablolu (Ethernet) aygıtı kablosuz router ile iletişim kuramıyor.

1. Köprünün tarayıcı tabanlı yardımcı programına erişin.
2. *Basic Wireless Settings* (Temel Kablosuz Ayarları) ekranında Network Name (SSID) (Ağ Adı (SSID)) seçeneğinin sizin kablosuz ağınızın adıyla eşleştiğinden emin olun.
3. Güvenlik ayarlarının (WPA, WPA2 veya WEP) kablosuz ağınızın güvenlik ayarlarıyla eşleştiğinden emin olun.

Köprünün IP adresinin değiştirilmesi gerekiyor.

Köprü ağa bir DHCP sunucusuyla (olağan durumda ağ router'ı) bağlıysa, köprü IP adresini DHCP sunucusundan alır. DHCP sunucusu yoksa, köprü varsayılan **169.254.1.250** statik IP adresini kullanır.

Köprünün her zaman statik bir IP adresi kullanmasını istiyorsanız şu yönergeleri uygulayın:

1. Köprünün tarayıcı tabanlı yardımcı programına erişin.
2. **Network Setup** (Ağ Ayarları) sekmesini tıklatın.
3. *Network Connection Type* (Ağ Bağlantısı Türü) açılır menüsünden **Static IP** (Statik IP) öğesini seçin.
4. *Static IP Address* (Statik IP Adresi), *Subnet Mask* (Alt-ağ Maskesi) ve *Default Gateway* (Varsayılan Ağ Geçidi) alanlarını doldurun.
5. **Save Settings** (Ayarları Kaydet) düğmesini tıklatın.

Köprü etkin bilgisayar veya diğer kablolu, Ethernet aygıtı başka bir kablosuz etkin aygıtla (bilgisayar veya yazıcı gibi) iletişim kurmuyor.

Aşağıdakileri kontrol edin:

- Kablosuz etkin aygıtın, bilgisayar veya diğer kablolu, Ethernet aygıtının köprüye bağlı olduğu aynı kablosuz ağda bulunduğundan emin olun.
- Kablosuz ağda tüm aygıtlar için aynı Network Name (SSID) (Ağ Adı (SSID)) kullanıldığından emin olun.
- Tüm aygıtların, uyumlu IP adreslerini kullanarak aynı IP ağında olduğundan emin olun.

Tarayıcı tabanlı yardımcı program parolanızı kabul etmiyor.

Aşağıdakileri kontrol edin:

- Parola büyük-küçük harf duyarlıdır. Parolayı girerken büyük/küçük harfleri doğru kullandığınızdan emin olun.
- Parolanızı unutursanız, köprüyü fabrika ayarlarına sıfırlayabilirsiniz.

 Köprünün **Reset** (Sıfırla) düğmesine yaklaşık beş saniye boyunca basın; parola fabrika varsayılan ayarına (**admin**) sıfırlanacaktır. Tüm diğer köprü ayarları da fabrika varsayılanlarına sıfırlanacaktır. (Tarayıcı tabanlı yardımcı programa girmek için, *Password* (Parola) alanına **admin** girin.

Tarayıcı tabanlı yardımcı programı kullanarak değişikliklerinizi yaptıktan sonra, yeni ayarlar ekranda gösterilmiyor.

Web tarayıcınızda, **Refresh** (Yenile) düğmesini tıklatın. Yeni ayarlar görüntülenmezse, bu yönergeleri uygulayın:

1. Köprüden güç adaptörü fişini çekin.
2. Beş saniye bekleyin ve güç adaptörü fişini köprüye geri takın.
3. Web tarayıcınızda, **Refresh** (Yenile) düğmesini tıklatın.

WEB
Sorularınızın yanıtını burada bulamıyorsanız **Linksys.com/support** adresindeki Linksys web sitesine bakın.

Spesifikasyonlar

WES610N

Model	WES610N
Standartlar	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED'ler	Güç, Ethernet, Wi-Fi Protected Setup™, Kablosuz, tek tek Ethernet bağlantısı ve etkinliği
Portlar	Ethernet (4), Güç
Düğmeler	Sıfırla, Wi-Fi Protected Setup
Kablo Türü	CAT5e
Antenler	3 (dahili)
Anten Konektör Tipi	-
Sökülebilir (Evet/Hayır)	Hayır
Modülasyonlar	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Gücü (EIRP) (dBm)	802.11a: 15 dBm (tipik) @ 54Mbps 802.11b: 19 dBm (tipik) @ 11 Mbps 802.11g: 16 dBm (tipik) @ 54 Mbps 802.11n (2.4 GHz): 18 dBm (tipik) @ 54 Mbps 802.11n (5 GHz): 16 dBm (tipik) @ MCS15
Alış Hassasiyeti	802.11a: -72 dBm (tipik) @ 54 Mbps 802.11b: –85 dBm (tipik) @ 11 Mbps 802.11g: -73 dBm (tipik) @ 54 Mbps 802.11n (20 MHz): -75 dBm (tipik) @ 54 Mbps 802.11n (40 MHz): -69 dBm (tipik) @ MCS15
dBi cinsinden Anten Kazancı	1
Kablosuz Güvenliği	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Güvenlik Anahtarı Bit Sayısı	128 bit şifrelemeye kadar

Çevresel

Boyutları	6,97" x 5,04" x 2,68" (177 x 128 x 68 mm)
Ağırlığı	0,65 lb (295 g)
Sertifikalar	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Güç	12V, 1A
Çalışma Sıcaklığı	32 - 104°F (0 - 40°C)
Depolama Sıcaklığı	-4 - 140°F (-20 - 60°C)
Çalışma Nem Oranı	% 10 - 85 arası, Yoğuşmasız
Depolama Nem Oranı	% 5 - 90 arası, Yoğuşmasız

Teknik özellikler bildirimde bulunulmaksızın değiştirilebilir.

WET610N

Model	WET610N
Standartlar	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
LED'ler	Güç, Ethernet, Wi-Fi Protected Setup™, Kablosuz
Portlar	Ethernet (4), Güç
Düğmeler	Sıfırla, Wi-Fi Protected Setup
Kablo Türü	CAT5e
Antenler	3 (dahili)
Anten Konektör Tipi	-
Sökülebilir (Evet/Hayır)	Hayır
Modülasyonlar	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
RF Gücü (EIRP) (dBm)	802.11a: 15 dBm (tipik) @ 54Mbps 802.11b: 18 dBm (tipik) @ 11 Mbps 802.11g: 16 dBm (tipik) @ 54 Mbps 802.11n: 12 dBm (tipik) @ 130 Mbps (HT20), 270 Mbps (HT40)
Alış Hassasiyeti	802.11a: -72 dBm (tipik) @ 54 Mbps 802.11b: –85 dBm (tipik) @ 11 Mbps 802.11g: -73 dBm (tipik) @ 54 Mbps 802.11n: -70 dBm (tipik) @ MCS15/2.4 GHz, -69 dBm (tipik) @ MCS15/5.0 GHz
dBi cinsinden Anten Kazancı	1
Kablosuz Güvenliği	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Güvenlik Anahtarı Bit Sayısı	128 bit şifrelemeye kadar

Çevresel

Boyutları	5,71" x 4,17" x 2,05" (145 x 106 x 52 mm)
Ağırlığı	5,61 oz (159 g)
Sertifikalar	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Güç	12V, 1A
Çalışma Sıcaklığı	32 - 104ºF (0 - 40ºC)
Depolama Sıcaklığı	-4 - 140°F (-20 - 60°C)
Çalışma Nem Oranı	% 10 - 85 arası, Yoğuşmasız
Depolama Nem Oranı	% 5 - 90 arası, Yoğuşmasız

Teknik özellikler bildirimde bulunulmaksızın değiştirilebilir.

Linksys.com/support

Cisco, Cisco logosu ve Linksys, Cisco ve/veya bağlı şirketlerinin ABD'de ve başka ülkelerdeki ticari markaları veya tescilli ticari markalarıdır.
Cisco'nun ticari markalarının bir listesi www.cisco.com/go/trademarks adresinde bulunabilir. Bu belgede belirtilen diğer tüm ticari markalar kendi sahiplerinin malıdır.

© 2011 Cisco ve/veya bağlı şirketleri. Tüm hakları saklıdır.

3425-01249



Посібник користувача

Linksys WET610N/WES610N

Мультимедійний міст подвійного діапазону для мереж стандарту N

Зміст

Огляд вибору

Панель світлодіодних індикаторів 2
Панель портів 3

Контрольний список для забезпечення захисту бездротового зв'язку

Зміна імені бездротової мережі (SSID) за замовчуванням 4
Зміна пароля за замовчуванням 4
Увімкнення фільтрування MAC-адрес 4
Увімкнення шифрування 4

Загальні правила захисту мереж 4
Додаткові поради з безпеки 5

Налаштування додаткових параметрів

Відкриття службової програми, що працює у браузері 6
Setup (Налаштування) > Basic Setup (Базове налаштування) . . . 7
Language (Мова) 7
Network Setup (Налаштування мережі) 7
Wireless (Бездротовий зв'язок) > Basic Wireless Settings (Базові налаштування бездротового зв'язку) 7
Basic Wireless Settings (Базові налаштування бездротового зв'язку) 8
Wireless Security (Захист бездротового зв'язку) 8
Wi-Fi Protected Setup (Захищене встановлення Wi-Fi) 9
Wireless (Бездротовий зв'язок) > Wireless Network Site Survey (Пошук локальних бездротових мереж) 10
Wireless Network Site Survey (Пошук локальних бездротових мереж) 10
Wireless (Бездротовий зв'язок) > WMM® 11
WMM 11
Wireless (Бездротовий зв'язок) > Basic Wireless Settings (Додаткові налаштування бездротового зв'язку) 13
Advanced Wireless (Додаткові налаштування бездротового зв'язку) 13
Administration (Адміністрування) > Management (Керування) 14
Management (Керування) 14
Administration (Адміністрування) > Factory Defaults (Заводські значення параметрів) 15
Factory Defaults (Заводські значення параметрів) 15
Administration (Адміністрування) > Upgrade Firmware (Оновлення мікропрограмного забезпечення) 15
Upgrade Firmware (Оновлення мікропрограмного забезпечення) 15
Status (Стан) > Bridge (Міст) 15
Bridge Information (Інформація про міст) 16
Local Network (Локальна мережа) 16
Status (Стан) > Wireless (Бездротовий зв'язок) 16
Wireless (Бездротовий зв'язок) 16

Усунення несправностей

WES610N/WET610N 17

Технічні характеристики

WES610N 18
WET610N 19

Огляд вибору

Дякуємо за придбання мультимедійного мосту подвійного діапазону Linksys для мереж стандарту N. Міст призначено для підключення будь-яких дротових пристроїв (пристроїв зі з'єднанням Ethernet) до бездротової мережі. В основі мосту лежить технологія бездротового зв'язку за стандартом N, тому він сумісний із будь-якими бездротовими маршрутизаторами або точками доступу, що відповідають стандартам бездротового зв'язку N, G, A або B. Для встановлення необхідно виконати інструкції, що містяться у папці на компакт-диску. Задати значення додаткових параметрів можна за допомогою зручної службової програми, що працює у браузері.

Панель світлодіодних індикаторів



WES610N

WET610N

Бездротовий зв'язок (синій) Цей індикатор світиться за наявності зв'язку із бездротовою мережею. Коли міст активно надсилає або приймає дані через бездротову мережу, цей індикатор блимає.

Кнопка Wi-Fi Protected Setup Якщо маршрутизатор підтримує функцію Wi-Fi Protected Setup і використовує захист за стандартом WPA або WPA2, міст можна підключити автоматично за допомогою зазначеної функції. Інструкції із використання функції Wi-Fi Protected Setup див. у розділі «Wireless (Бездротовий зв'язок) > Basic Wireless Settings (Базові налаштування бездротового зв'язку)» на стор. 7.

Індикатор Wi-Fi Protected Setup (синій/оранжевий) Індикатор блимає синім кольором упродовж двох хвилин під час виконання функції Wi-Fi Protected Setup. Коли захист бездротового зв'язку увімкнено, індикатор неперервно світиться синім кольором. Якщо під час виконання функції Wi-Fi Protected Setup сталася помилка, індикатор світиться оранжевим кольором. Переконайтеся в тому, що маршрутизатор підтримує функцію Wi-Fi Protected Setup. Дочекайтеся, доки індикатор не згасне, а потім повторіть спробу.

Ethernet (синій) Індикатор Ethernet світиться за наявності дротового з'єднання. Коли міст активно надсилає або приймає дані через з'єднання Ethernet, цей індикатор блимає.

Живлення (синій) Цей індикатор світиться, коли на міст подається електричне живлення.

Панель портів



WES610N WET610N

Ethernet Порти Ethernet служать для підключення моста до комп'ютера або інших дротових мережевих пристроїв. На моделі WES610N чотири таких порти, на моделі WET610N — один.

Reset (Скидання) Відновити заводські значення параметрів моста можна у два способи. Натисніть і утримуйте близько п'яти секунд кнопку Reset (Скидання) або відновіть значення за замовчуванням з екрана Administration (Адміністрування) > Factory Defaults (Заводські значення параметрів). У моделі WES610N кнопка скидання розташована на нижній панелі, у моделі WET610N — на задній панелі портів.

Живлення До цього порту підключається адаптер живлення, що входить до комплекту поставки мосту.

Контрольний список для забезпечення захисту бездротового зв'язку

Бездротові мережі зручні у використанні та легко встановлюються, тому їх дедалі частіше використовують для забезпечення швидкого доступу до Інтернету. У бездротових мережах дані надсилаються радіохвилями, тому вони вразливіші для перехоплення, аніж дані у традиційних дротових мережах. Сигнали бездротових мереж можуть перехоплюватися так само, як сигнали мобільних або бездротових телефонів. Оскільки неможливо запобігти фізичному підключенню інших користувачів до бездротової мережі, необхідно вжити додаткових заходів для її захисту.

Зміна імені бездротової мережі (SSID) за замовчуванням

Кожен бездротовий пристрій має заводський ідентифікатор набору служб (Service Set Identifier, SSID). Це ім'я відповідної бездротової мережі, яке може містити до 32 символів. У виробах Linksys використовується заводське ім'я бездротової мережі **linksys**. Заводське ім'я бездротової мережі необхідно змінити. Воно має бути унікальним і надавати змогу відрізнити цю мережу від інших бездротових мереж, що можуть бути наявні поруч. Не рекомендується використовувати особисті дані (на кшталт ідентифікаційного коду), оскільки ці дані будуть доступні для всіх користувачів, які шукатимуть бездротові мережі.

Зміна пароля за замовчуванням

Доступ до зміни значень параметрів бездротових виробів на кшталт точок доступу та маршрутизаторів захищений паролем. Пароль за замовчуванням задається на цих виробах на заводі. У виробах Linksys використовується пароль за замовчуванням **admin**. Ці заводські значення добре відомі хакерам, які можуть скористатися ними для доступу до бездротового пристрою та зміни значень параметрів мережі. Для запобігання несанкціонованим змінам необхідно захистити пристрій унікальним паролем, який буде важко підібрати.

Увімкнення фільтрування MAC-адрес

На маршрутизаторах Linksys можна ввімкнути фільтрування адрес керування мультимедійним доступом (Media Access Control, MAC). MAC-адреса — це набір цифр і букв, унікальний для кожного мережевого пристрою. Коли увімкнено фільтрування MAC-адрес, доступ до бездротової мережі надається лише бездротовим пристроям із певними MAC-адресами. Наприклад, можна вказати MAC-адреси всіх комп'ютерів у помешканні, щоб доступ до бездротової мережі мали лише ці комп'ютери.

Увімкнення шифрування

Шифрування захищає дані, що передаються бездротовою мережею. Стандарти захищеного доступу Wi-Fi (Wi-Fi Protected Access, WPA/WPA2) та конфіденційності на рівні дротових мереж (Wired Equivalent Privacy, WEP) забезпечують різні рівні захисту бездротового зв'язку.

Шифрування даних у мережі за допомогою стандарту WPA/WPA2 безпечніше, аніж за допомогою стандарту WEP, оскільки у WPA/WPA2 для шифрування використовується динамічний ключ. Для захисту даних під час бездротового передавання необхідно ввімкнути максимальний рівень шифрування, що підтримується мережевим обладнанням.

WEP — це дещо старіший стандарт. На деяких старих пристроях, які не підтримують WPA, може бути доступним лише він.

Загальні правила захисту мереж

Немає сенсу вживати заходів для захисту бездротової мережі, якщо мережа, що лежить в основі бездротової, не є безпечною.

- Захистіть паролями всі комп'ютери, що входять до мережі, та окремо захистіть паролем усі конфіденційні файли.
- Регулярно змінюйте паролі.
- Установіть антивірусне програмне забезпечення та брандмауери для особистого використання.
- Забороніть рівноправний спільний доступ до даних (обмін даними) між пристроями. Деякі програми можуть дозволяти спільний доступ до файлів без згоди та (або) відома користувача.

Додаткові поради з безпеки

- Не розташовуйте бездротові маршрутизатори, точки доступу або шлюзи на зовнішніх стінах та поблизу вікон.
- Вимикайте бездротові маршрутизатори, точки доступу або шлюзи, коли вони не використовуються (уночі, на час відпустки).
- Вибирайте надійні паролі, що містять не менше восьми символів. Комбінуйте букви та цифри, щоб уникнути використання стандартних слів, наявних у словнику.

Налаштування додаткових параметрів

Після виконання інструкцій з налаштування моста, наведених у папці на компакт-диску, міст буде готовий до використання. Однак щоб змінити значення додаткових параметрів, необхідно скористатися службовою програмою моста, що працює у браузері. У цьому розділі розглядаються всі веб-сторінки цієї службової програми та відповідні основні функції. Відкрити службову програму можна із веб-браузера на комп'ютері, підключеного до мережі цього моста.

У службовій програмі, що працює у браузері, є такі основні вкладки: Setup (Налаштування), Wireless (Бездротовий зв'язок), Administration (Адміністрування) та Status (Стан). Додаткові вкладки відображаються після переходу на одну з основних вкладок.

Відкриття службової програми, що працює у браузері

Для відкриття службової програми, що працює у браузері, слід скористатися веб-браузером.

Якщо міст підключений до мережі із DHCP-сервером (зазвичай через мережевий маршрутизатор), міст отримує IP-адресу від DHCP-сервера. Якщо DHCP-сервер відсутній, міст використовуватиме статичну IP-адресу за замовчуванням: **169.254.1.250**. (Якщо постійна статична IP-адреса надається мосту за допомогою службової програми, що працює у браузері, введіть нову IP-адресу замість зазначеної.)

ПРИМІТКА
Якщо ви не знаєте IP-адресу моста, знайдіть її у таблиці DHCP-клієнтів на маршрутизаторі. (Див. документацію на маршрутизатор.)

Якщо знайти IP-адресу моста не вдається, можна скинути налаштовані значення його параметрів. Натисніть і утримуйте близько п'яти секунд кнопку **Reset** (Скидання) на мості за допомогою розпрямленої канцелярської скріпки. Це призведе до відновлення заводських значень параметрів моста. Міст запитає IP-адресу в DHCP-сервера (зазвичай – мережевого маршрутизатора). Якщо DHCP-сервер не знайдено, міст використовує статичну IP-адресу за замовчуванням: **169.254.1.250**, доки не знайде DHCP-сервер і не отримає динамічну IP-адресу.

Якщо міст не пов'язаний із маршрутизатором і на ньому встановлено заводські значення параметрів, підключіть до моста комп'ютер через з'єднання Ethernet, щоб отримати доступ до службової програми, що працює у браузері. З'єднання Ethernet потрібно налаштувати на комп'ютері, указавши статичну IP-адресу та маску підмережі.

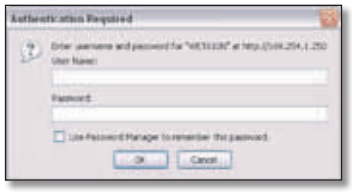
На адаптері Ethernet необхідно задати конкретну IP-адресу.

1. Введіть до поля *IP-адреса* значення **169.254.x.y** (замість x необхідно ввести число від 1 до 254, замість y — число від 0 до 255).
2. У поле *Маска підмережі* введіть значення **255.255.0.0**.

ПРИМІТКА
Дії з надання статичної IP-адреси адаптеру Ethernet на комп'ютері можуть різнитися залежно від операційної системи. Докладні інструкції див. у довідковій документації конкретної операційної системи.

Надавши адаптеру Ethernet статичну IP-адресу, запустіть веб-браузер і введіть цю IP-адресу (значення за замовчуванням: **169.254.1.250**) до *адресного рядка*. Натисніть клавішу **Enter**.

Відобразиться екран запиту пароля. (В інших операційних системах, аніж Windows XP, відображається подібний екран.) Залиште поле *Ім'я користувача* порожнім. Введіть пароль, створений під час виконання майстра налаштування. Якщо новий пароль не створено, введіть пароль за замовчуванням: **admin**. (Задати новий пароль можна на екрані *Administration (Адміністрування)* > *Management (Керування)*.) Натисніть **OK**, щоб продовжити.



ПРИМІТКА
Якщо екран запиту пароля не відобразиться, зачекайте дві хвилини та повторіть спробу.

Setup (Налаштування) > Basic Setup (Базове налаштування)

Першим відображається екран *Basic Setup* (Базове налаштування). На цьому екрані можна вибрати мову службової програми, що працює у браузері, або змінити значення параметрів дротової мережі (Ethernet) моста.





Language (Мова)

Language (Мова) Тут можна вибрати мову інтерфейсу користувача службової програми, що працює у браузері. Виберіть потрібну мову із розкривного списку.

Network Setup (Налаштування мережі)

Значення параметрів цього розділу визначають, чи отримує міст IP-адресу від DHCP-сервера (на кшталт мережевого маршрутизатора) автоматично (Automatic Configuration — DHCP (Автоматичне конфігурування — DHCP)), або ж IP-адреса задається вручну (Static IP (Статична IP-адреса)).

Bridge IP (IP-адреса моста) Якщо в мережі є DHCP-сервер на кшталт мережевого маршрутизатора, що надає IP-адреси мережевим пристроям, залиште значення за замовчуванням: **Automatic Configuration — DHCP** (Автоматичне конфігурування — DHCP). Міст запитає IP-адресу в DHCP-сервера (зазвичай це мережевий маршрутизатор). Якщо DHCP-сервер не знайдено, міст використовуватиме статичну IP-адресу за замовчуванням: **169.254.1.250**, доки не знайде DHCP-сервер і не отримає динамічну IP-адресу.

Щоб задати постійну статичну IP-адресу моста, виберіть значення **Static IP** (Статична IP-адреса).

Якщо вибрано значення Static IP (Статична IP-адреса), слід заповнити наведені нижче поля.

- **Static IP Address** (Статична IP-адреса) Введіть унікальну IP-адресу, яка використовуватиметься для доступу до службової програми, що працює у браузері.
- **Subnet Mask** (Маска підмережі) Введіть адресу маски підмережі дротової мережі.
- **Default Gateway** (Шлюз за замовчуванням) Введіть IP-адресу мережевого шлюзу за замовчуванням (у більшості випадків це маршрутизатор).

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Wireless (Бездротовий зв'язок) > Basic Wireless Settings (Базові налаштування бездротового зв'язку)

На екрані *Basic Wireless Settings* (Базові налаштування бездротового зв'язку) можна задати значення базових параметрів моста, які керують здійсненням бездротового зв'язку.

Є два способи налаштування значень параметрів моста: вручну та за допомогою функції Wi-Fi Protected Setup (Захищене встановлення Wi-Fi). Wi-Fi Protected Setup (Захищене встановлення Wi-Fi) — це функція, яка спрощує налаштування бездротової мережі. Якщо мережевий маршрутизатор підтримує функцію Wi-Fi Protected Setup (Захищене встановлення Wi-Fi) та використовує стандарт безпеки WPA або WPA2, то за допомогою функції Wi-Fi Protected Setup (Захищене встановлення Wi-Fi) можна автоматично підключити міст.

Configuration View (Перегляд конфігурації) Щоб налаштувати бездротову мережу вручну, виберіть значення **Manual** (Вручну). Див. розділ **Basic Wireless Settings (Базові налаштування бездротового зв'язку)**, **стор. 8**. Щоб скористатися функцією Wi-Fi Protected Setup (Захищене встановлення Wi-Fi), виберіть значення **Wi-Fi Protected Setup**. Див. розділ **Wi-Fi Protected Setup (Захищене встановлення Wi-Fi)**, **стор. 9**.

Basic Wireless Settings (Базові налаштування бездротового зв'язку)



Network Name (SSID) (Ім'я мережі (SSID)) SSID — це ім'я мережі, спільне для всіх точок бездротової мережі. Ім'я SSID має бути однаковим на всіх пристроях, які входять до бездротової мережі. Воно чутливе до регістру та має містити не більше 32 символів (допускаються будь-які символи, наявні на клавіатурі). Переконайтеся в тому, що значення цього параметра відповідає значенню аналогічного параметра на бездротовому маршрутизаторі або точці доступу. Для підвищення рівня безпеки слід змінити ім'я SSID за замовчуванням (**linksys**) на унікальне ім'я.

Wireless Security (Захист бездротового зв'язку)

Міст підтримує такі можливості захисту бездротового зв'язку: WPA Personal (Індивідуальний WPA), WPA2 Personal (Індивідуальний WPA2) та WEP. WPA (Wi-Fi Protected Access — захищений доступ Wi-Fi) та WPA2 є надійнішими методами забезпечення захисту, аніж WEP (Wired Equivalent Privacy — конфіденційність на рівні дротових мереж). Докладніше про захист бездротового зв'язку див. у розділі «Контрольний список для забезпечення захисту бездротового зв'язку» на стор. 4.

Security Mode (Режим захисту)

Виберіть режим захисту бездротової мережі. Щоб відмовитися від захисту бездротового зв'язку, залиште незмінним значення за замовчуванням: **Disabled** (Вимкнено).

ПРИМІТКА
Пам'ятайте, що на всіх пристроях у бездротовій мережі МАЮТЬ використовуватися той самий метод захисту та той самий пароль/ключ. В іншому разі бездротові пристрої не зможуть здійснювати обмін даними.

WPA Personal (Індивідуальний WPA)

WPA — це стандарт захисту, надійніший за шифрування WEP.



Encryption (Шифрування) WPA підтримує метод шифрування TKIP, в якому використовуються динамічні шифрувальні ключі.

Passphrase (Пароль) Введіть пароль, спільний для моста та бездротового маршрутизатора або точки доступу. Він має містити від 8 до 63 символів.

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

WPA2 Personal (Індивідуальний WPA2)

WPA2 — це більш сучасна та надійна версія стандарту WPA.



Encryption (Шифрування) WPA2 підтримує два методи шифрування: TKIP та AES, у яких використовуються динамічні шифрувальні ключі. Виберіть метод шифрування: **AES** або **TKIP or AES** (TKIP або AES). За замовчуванням вибрано значення **AES**.

Passphrase (Пароль) Введіть пароль, спільний для моста та бездротового маршрутизатора або точки доступу. Він має містити від 8 до 63 символів.

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

WEP

WEP — це базовий метод шифрування, менш надійний, аніж WPA або WPA2.



Encryption (Шифрування) Виберіть рівень шифрування WEP: **40/64 bits (10 hex digits)** (40/64 біт (10 шістнадцяткових цифр)) або **104/128 bits (26 hex digits)** (104/128 біт (26 шістнадцяткових цифр)). Значення за замовчуванням: **40/64 bits (10 hex digits)** (40/64 біт (10 шістнадцяткових цифр)).

Key 1 (Ключ 1) Введіть ключ WEP мережі.

Tx Key (Ключ передавання) **Key 1** (Ключ 1) — ключ передавання, що використовується мостом.

Authentication (Аутентифікація) Значення за замовчуванням: **Auto** (Автоматично). Воно дає змогу використовувати аутентифікацію за методом відкритої системи або спільного ключа. Виберіть значення **Open** (Відкрита), щоб увімкнути аутентифікацію за методом відкритої системи. Передавач і приймач даних не використовуватимуть ключ WEP для аутентифікації. Виберіть значення **Shared** (Спільна), щоб увімкнути аутентифікацію за методом спільного ключа. Передавач і приймач даних використовуватимуть ключ WEP для аутентифікації.

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Wi-Fi Protected Setup (Захищене встановлення Wi-Fi)

Існує два способи використання цієї функції. Виберіть спосіб, який відповідає наявному маршрутизатору.





Спосіб 1

Цим способом можна скористатися, якщо маршрутизатор має кнопку Wi-Fi Protected Setup (Захищене встановлення Wi-Fi).

1. Натисніть екранну або фізичну кнопку **Wi-Fi Protected Setup** (Захищене встановлення Wi-Fi) на маршрутизаторі.
2. Упродовж двох хвилин натисніть кнопку **Wi-Fi Protected Setup** (Захищене встановлення Wi-Fi) на екрані *Wi-Fi Protected Setup* маршрутизатора.
3. Після того, як параметри моста буде сконфігуровано, натисніть **Close** (Закрити).

На екрані *Wi-Fi Protected Setup* (Захищене встановлення Wi-Fi) відображаються такі параметри: Link Status (Стан каналу), Network Name (SSID) (Ім'я мережі (SSID)), а також метод захисту.

Спосіб 2

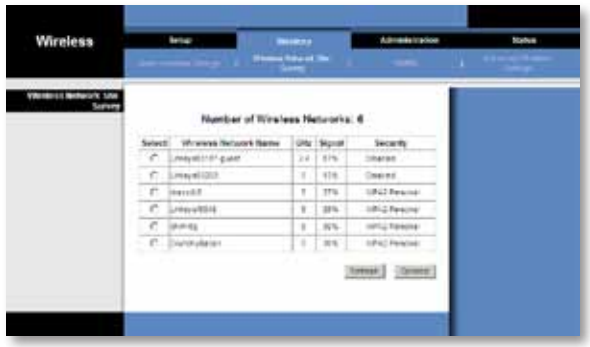
Скористайтеся цим способом, якщо маршрутизатор запитає PIN-код моста.

1. На екрані **маршрутизатора** *Wi-Fi Protected Setup* (Захищене встановлення Wi-Fi) введіть PIN-код, відображений на однойменному екрані **моста** . Потім натисніть кнопку **Register** (Зареєструвати) або іншу відповідну кнопку. (Цю інформацію також зазначено на наклейці з нижнього боку моста.)
2. На екрані **моста** *Wi-Fi Protected Setup* (Захищене встановлення Wi-Fi) натисніть кнопку **OK**.
3. Після того, як параметри моста буде сконфігуровано, натисніть **Close** (Закрити).

На екрані *Wi-Fi Protected Setup* (Захищене встановлення Wi-Fi) відображаються такі параметри: Link Status (Стан каналу), Network Name (SSID) (Ім'я мережі (SSID)), а також метод захисту.

Wireless (Бездротовий зв'язок) > Wireless Network Site Survey (Пошук локальних бездротових мереж)

Відкрийте вкладку **Wireless Network Site Survey** (Пошук локальних бездротових мереж), щоб почати пошук локальних бездротових мереж. На екрані *Wireless Network Site Survey* (Пошук локальних бездротових пристроїв) наведено список локальних бездротових мереж, знайдених мостом.



Wireless Network Site Survey (Пошук локальних бездротових мереж)

Number of Wireless Networks (Кількість бездротових мереж) Відображається кількість бездротових мереж, знайдених мостом.

Select (Вибрати) Щоб підключити міст до мережі, натисніть кнопку **Select** (Вибрати). Потім натисніть **Connect** (Підключити).

Wireless Network Name (Ім'я бездротової мережі) Відображається ім'я бездротової мережі (ідентифікатор SSID).

GHz (ГГц) Відображається діапазон радіочастот бездротової мережі.

Signal (Сигнал) Відображається рівень сигналу в процентах. Значення 100 % відповідає максимальному рівню сигналу; 0 % — мінімальному.

Security (Захист) Якщо мережа підтримує функцію Wi-Fi Protected Setup (Захищене встановлення Wi-Fi), відображається значок цієї функції . Відображається метод захисту, використовуваний бездротовою мережею.

Натисніть **Refresh** (Оновити), щоб оновити інформацію на екрані.

Вибравши мережу, натисніть **Connect** (Підключити). Відобразиться новий екран. Виконайте інструкції з налаштування методу безпеки відповідної мережі.

WPA



Network Name (SSID) (Ім'я мережі (SSID)) Автоматично відображається ім'я вибраної мережі.

Security Mode (Режим захисту) Автоматично відображається режим WPA Personal (Індивідуальний WPA).

Encryption (Шифрування) WPA підтримує метод шифрування TKIP, в якому використовуються динамічні шифрувальні ключі.

Passphrase (Пароль) Введіть пароль, спільний для моста та бездротового маршрутизатора або точки доступу. Він має містити від 8 до 63 символів.

Натисніть **Refresh** (Оновити), щоб оновити інформацію на екрані.

Ввівши значення параметрів захисту, натисніть **Connect** (Підключити).

WPA2



Network Name (SSID) (Ім'я мережі (SSID)) Автоматично відображається ім'я вибраної мережі.

Security Mode (Режим захисту) Автоматично відображається режим WPA2 Personal (Індивідуальний WPA2).

Encryption (Шифрування) WPA2 підтримує два методи шифрування: TKIP та AES, у яких використовуються динамічні шифрувальні ключі. Виберіть метод шифрування: **AES** або **TKIP or AES** (TKIP або AES).

Passphrase (Пароль) Введіть пароль, спільний для моста та бездротового маршрутизатора або точки доступу. Він має містити від 8 до 63 символів.

Натисніть **Refresh** (Оновити), щоб оновити інформацію на екрані.

Ввівши значення параметрів захисту, натисніть **Connect** (Підключити).

WEP



Network Name (SSID) (Ім'я мережі (SSID)) Автоматично відображається ім'я вибраної мережі.

Security Mode (Режим захисту) Автоматично відображається WEP.

Encryption (Шифрування) Виберіть рівень шифрування WEP: **40/64 bits (10 hex digits)** (40/64 біт (10 шістнадцяткових цифр)) або **104/128 bits (26 hex digits)** (104/128 біт (26 шістнадцяткових цифр)).

Key 1 (Ключ 1) Введіть ключ WEP мережі.

Tx Key (Ключ передавання) **Key 1** (Ключ 1) — ключ передавання, що використовується мостом.

Authentication (Аутентифікація) Значення за замовчуванням: **Auto** (Автоматично). Воно дає змогу використовувати аутентифікацію за методом відкритої системи або спільного ключа. Виберіть значення **Open** (Відкрита), щоб увімкнути аутентифікацію за методом відкритої системи. Передавач і приймач даних не використовуватимуть ключ WEP для аутентифікації. Виберіть значення **Shared** (Спільна), щоб увімкнути аутентифікацію за методом спільного ключа. Передавач і приймач даних використовуватимуть ключ WEP для аутентифікації.

Натисніть **Refresh** (Оновити), щоб оновити інформацію на екрані.

Ввівши значення параметрів захисту, натисніть **Connect** (Підключити).

Wireless (Бездротовий зв'язок) > WMM®

Задайте значення параметрів мультимедійного бездротового зв'язку — Wireless MultiMedia (WMM). Стандарт WMM забезпечує визначення пріоритетів пакетів залежно від режиму доступу (типу трафіку): Background (Фоновий), Best Effort (Найкраще з доступного), Video (Відео) або Voice (Голос). Змінювати значення цих параметрів дозволяється лише компетентним адміністраторам, адже неправильна конфігурація може погіршити продуктивність бездротового зв'язку.



ПРИМІТКА
Параметри на екрані *WMM* призначені лише для досвідчених користувачів.

WMM

Access Mode (Режим доступу)

Можна задати різні значення параметрів чотирьох доступних режимів доступу. Виберіть режим, який потрібно сконфігурувати: **Background** (Фоновий), **Best Effort** (Найкраще з доступного), **Video** (Відео) або **Voice** (Голос). Виконайте інструкції для вибраного режиму.

Background (Фоновий)

Use Aggregation (Використовувати агрегування) Цей параметр визначає, чи має рівень керування мультимедійним доступом (Media Access Control, MAC) починати сеанс додавання підтвердження блоків (Add Block Acknowledgement, ADDBA). Значення за замовчуванням: **No** (Ні). Виберіть **Yes** (Так), щоб увімкнути цю функцію.

Accept Aggregation (Приймати агрегування) Цей параметр визначає, чи прийматиме рівень MAC запити ADDBA. Значення за замовчуванням: **Yes** (Так). Виберіть **No** (Ні), щоб вимкнути цю функцію.

Max. Number of Packets in Aggregation (Макс. кількість пакетів у агрегаті) Цей параметр визначає максимальну кількість пакетів (підблоків даних) у сукупності даних. Діапазон значень: від **0** до **7**. Значення за замовчуванням: **7**.

Max. Aggregation Size (Макс. розмір агрегату) Цей параметр визначає максимальний розмір агрегату (в байтах). Діапазон значень: від **0** до **16000**. Значення за замовчуванням: **12000**.

Timeout Internal (Внутрішній час очікування) Цей параметр визначає час очікування, упродовж якого агрегат має бути закритий «умовою закриття», перш ніж його буде закрито таймером. Діапазон значень: від **0** до **100**. Значення за замовчуванням: **3**.

Min. Size of Packet in Aggregation (Мін. розмір пакета в агрегаті) Цей параметр визначає мінімальний розмір (у байтах) пакетів, які накопичуються в агрегаті. Діапазон значень: від **0** до **1500**. Значення за замовчуванням: **10**.

ADDBA Timeout (Час очікування ADDBA) Цей параметр визначає період часу, після спливу якого сеанс ADDBA припиняється за умови, що впродовж цього періоду відсутній обмін блоками даних у рамках узгодженого підтвердження блоків (ACK). Діапазон значень: від **0** до **65535**. Значення за замовчуванням: **0**, тобто час очікування відсутній.

Aggregation Window Size (Розмір вікна агрегування) Цей параметр визначає максимальну кількість пакетів, які можуть бути передані без отримання підтверджень ACK. Діапазон значень: від **0** до **64**. Значення за замовчуванням: **64**.

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Best Effort (Найкраще з доступного)

Use Aggregation (Використовувати агрегування) Цей параметр визначає, чи має рівень керування мультимедійним доступом (Media Access Control, MAC) починати сеанс додавання підтвердження блоків (Add Block Acknowledgement, ADDBA). Значення за замовчуванням: **Yes** (Так). Виберіть **No** (Ні), щоб вимкнути цю функцію.

Accept Aggregation (Приймати агрегування) Цей параметр визначає, чи прийматиме рівень MAC запити ADDBA. Значення за замовчуванням: **Yes** (Так). Виберіть **No** (Ні), щоб вимкнути цю функцію.

Max. Number of Packets in Aggregation (Макс. кількість пакетів у агрегаті) Цей параметр визначає максимальну кількість пакетів (підблоків даних) у сукупності даних. Діапазон значень: від **0** до **10**. Значення за замовчуванням: **10**.

Max. Aggregation Size (Макс. розмір агрегату) Цей параметр визначає максимальний розмір агрегату (в байтах). Діапазон значень: від **0** до **20000**. Значення за замовчуванням: **16000**.

Timeout Internal (Внутрішній час очікування) Цей параметр визначає час очікування, упродовж якого агрегат має бути закритий «умовою закриття», перш ніж його буде закрито таймером. Діапазон значень: від **0** до **100**. Значення за замовчуванням: **3**.

Min. Size of Packet in Aggregation (Мін. розмір пакета в агрегаті) Цей параметр визначає мінімальний розмір (у байтах) пакетів, які накопичуються в агрегаті. Діапазон значень: від **0** до **1500**. Значення за замовчуванням: **10**.

ADDBA Timeout (Час очікування ADDBA) Цей параметр визначає період часу, після спливу якого сеанс ADDBA припиняється за умови, що впродовж цього періоду відсутній обмін блоками даних у рамках узгодженого підтвердження блоків (ACK). Діапазон значень: від **0** до **65535**. Значення за замовчуванням: **0**, тобто час очікування відсутній.

Aggregation Window Size (Розмір вікна агрегування) Цей параметр визначає максимальну кількість пакетів, які можуть бути передані без отримання підтверджень ACK. Діапазон значень: від **0** до **64**. Значення за замовчуванням: **64**.

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Video (Відео)

Use Aggregation (Використовувати агрегування) Цей параметр визначає, чи має рівень керування мультимедійним доступом (Media Access Control, MAC) починати сеанс додавання підтвердження блоків (Add Block Acknowledgement, ADDBA). Значення за замовчуванням: **Yes** (Так). Виберіть **No** (Ні), щоб вимкнути цю функцію.

Accept Aggregation (Приймати агрегування) Цей параметр визначає, чи прийматиме рівень MAC запити ADDBA. Значення за замовчуванням: **Yes** (Так). Виберіть **No** (Ні), щоб вимкнути цю функцію.

Max. Number of Packets in Aggregation (Макс. кількість пакетів у агрегаті) Цей параметр визначає максимальну кількість пакетів (підблоків даних) у сукупності даних. Діапазон значень: від **0** до **7**. Значення за замовчуванням: **7**.

Max. Aggregation Size (Макс. розмір агрегату) Цей параметр визначає максимальний розмір агрегату (в байтах). Діапазон значень: від **0** до **16000**. Значення за замовчуванням: **12000**.

Timeout Internal (Внутрішній час очікування) Цей параметр визначає час очікування, упродовж якого агрегат має бути закритий «умовою закриття», перш ніж його буде закрито таймером. Діапазон значень: від **0** до **100**. Значення за замовчуванням: **3**.

Min. Size of Packet in Aggregation (Мін. розмір пакета в агрегаті) Цей параметр визначає мінімальний розмір (у байтах) пакетів, які накопичуються в агрегаті. Діапазон значень: від **0** до **1500**. Значення за замовчуванням: **10**.

ADDBA Timeout (Час очікування ADDBA) Цей параметр визначає період часу, після спливу якого сеанс ADDBA припиняється за умови, що впродовж цього періоду відсутній обмін блоками даних у рамках узгодженого підтвердження блоків (ACK). Діапазон значень: від **0** до **65535**. Значення за замовчуванням: **0**, тобто час очікування відсутній.

Aggregation Window Size (Розмір вікна агрегування) Цей параметр визначає максимальну кількість пакетів, які можуть бути передані без отримання підтверджень ACK. Діапазон значень: від **0** до **64**. Значення за замовчуванням: **64**.

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Voice (Голос)

Use Aggregation (Використовувати агрегування) Цей параметр визначає, чи має рівень керування мультимедійним доступом (Media Access Control, MAC) починати сеанс додавання підтвердження блоків (Add Block Acknowledgement, ADDBA). Значення за замовчуванням: **Yes** (Так). Виберіть **No** (Ні), щоб вимкнути цю функцію.

Accept Aggregation (Приймати агрегування) Цей параметр визначає, чи прийматиме рівень MAC запити ADDBA. Значення за замовчуванням: **Yes** (Так). Виберіть **No** (Ні), щоб вимкнути цю функцію.

Max. Number of Packets in Aggregation (Макс. кількість пакетів у агрегаті) Цей параметр визначає максимальну кількість пакетів (підблоків даних) у сукупності даних. Діапазон значень: від **0** до **2**. Значення за замовчуванням: **2**.

Max. Aggregation Size (Макс. розмір агрегату) Цей параметр визначає максимальний розмір агрегату (в байтах). Діапазон значень: від **0** до **16000**. Значення за замовчуванням: **10000**.

Timeout Internal (Внутрішній час очікування) Цей параметр визначає час очікування, упродовж якого агрегат має бути закритий «умовою закриття», перш ніж його буде закрито таймером. Діапазон значень: від **0** до **100**. Значення за замовчуванням: **10**.

Min. Size of Packet in Aggregation (Мін. розмір пакета в агрегаті) Цей параметр визначає мінімальний розмір (у байтах) пакетів, які накопичуються в агрегаті. Діапазон значень: від **0** до **1500**. Значення за замовчуванням: **10**.

ADDBA Timeout (Час очікування ADDBA) Цей параметр визначає період часу, після спливу якого сеанс ADDBA припиняється за умови, що впродовж цього періоду відсутній обмін блоками даних у рамках узгодженого підтвердження блоків (ACK). Діапазон значень: від **0** до **65535**. Значення за замовчуванням: **0**, тобто час очікування відсутній.

Aggregation Window Size (Розмір вікна агрегування) Цей параметр визначає максимальну кількість пакетів, які можуть бути передані без отримання підтверджень ACK. Діапазон значень: від **0** до **64**. Значення за замовчуванням: **64**.

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Wireless (Бездротовий зв'язок) > Basic Wireless Settings (Додаткові налаштування бездротового зв'язку)

Тут можна задати конфігурацію додаткових функцій моста, призначених для бездротового зв'язку. Змінювати значення цих параметрів дозволяється лише компетентним адміністраторам, адже неправильна конфігурація може погіршити продуктивність бездротового зв'язку.



ПРИМІТКА
Параметри на екрані *Advanced Wireless Settings* (Додаткові налаштування бездротового зв'язку) призначені лише для досвідчених користувачів.

Advanced Wireless (Додаткові налаштування бездротового зв'язку)

Use LDPC (Використовувати LDPC) Код із малою щільністю перевірок на парність (Low-Density Parity-Check Code, LDPC) дає змогу ввімкнути або вимкнути коригування помилок, щоб зменшити вірогідність утрати даних у каналах із високим рівнем перешкод. Алгоритм адаптування швидкості автоматично вимикає кодування LDPC під час роботи на високій швидкості PHY (вище за 162). Щоб використовувати передову схему коригування помилок LDCP, залиште значення за замовчуванням **Yes** (Так). В іншому разі виберіть **No** (Ні).

ERP Protection Type (Тип захисту ERP) Цей параметр конфігурує захист пакетів OFDM, незважаючи на наявність у бездротовій мережі станцій, які відповідають стандарту 802.11b. Передаючи пакети RTS/CTS або CTS2Self на швидкості, визначеній стандартом 802.11b, міст інформує бездротову мережу про те, що планується передавання пакетів OFDM, і захищає пакети в бездротовій мережі. Пакети RTS/CTS і CTS2Self створюють службові сигнали, що може призвести до зниження пропускної здатності.

Тип RTS/CTS забезпечує краще покриття, але гіршу пропускну спроможність порівняно із типом CTS2Self, оскільки RTS/CTS передбачає підтвердження з боку пристрою-отримувача. Щоб використовувати RTS/CTS, залиште значення за замовчуванням: **RTS/CTS**. Якщо не вибрати жодного типу, можливі конфлікти між пакетами OFDM і CCK. Щоб не вибирати жодного типу, виберіть **None** (Жодний). Щоб використовувати CTS2Self, виберіть значення **CTS2Self**.

11n Protection Type (Тип захисту 11n) Цей параметр визначає захист від пристроїв із низькою пропускною спроможністю, які входять у бездротову мережу. Якщо бездротовий маршрутизатор (або точка доступу) знаходить прив'язку до застарілого пристрою з низькою пропускною спроможністю, на всі пристрої з високою пропускною спроможністю передається сигнал про необхідність використання механізмів RTS/CTS або CTS2Self перед кожним передаванням даних. Ця функція також підтримує всі методи захисту згідно зі стандартом 802.11n, у тому числі MIMO.

Тип RTS/CTS забезпечує краще покриття, але гіршу пропускну спроможність порівняно із типом CTS2Self, оскільки RTS/CTS передбачає підтвердження з боку пристрою-отримувача. Щоб використовувати RTS/CTS, залиште значення за замовчуванням: **RTS/CTS**. Якщо не вибрати жодного типу, можливі конфлікти між пакетами HT і застарілими пакетами. Щоб не вибирати жодного типу, виберіть **None** (Жодний). Щоб використовувати CTS2Self, виберіть значення **CTS2Self**.

Percentage of maximal transmit power (Відсоток від максимальної потужності передавання) Цей параметр визначає рівень потужності передавання у відсотках від максимального рівня залежно від чинних регуляторних обмежень. Наприклад, якщо чинні регуляторні обмеження дозволяють передавання сигналу до 20 дБ, то після вибору значення 50 % максимальна дозволена потужність передавання становитиме 10 дБ. Виберіть потрібний відсоток: **12 %**, **25 %**, **50 %** або **100 %**. Значення за замовчуванням: **100 %**.

QoS Classification Type (Тип класифікації рівня обслуговування) Цей параметр прив'язує стандарти 802.1D або 802.1Q зі сфери IP DSCP/TOS до пріоритетів WMM (Background (Фоновий), Best Efforts (Найкраще з доступного), Video (Відео), Voice (Голос)). Залиште значення за замовчуванням, **802.1D** або виберіть значення **802.1Q**, яке використовується деякими потоками IPTV.

Re-establish Ethernet connection when initiating wireless connection (Перевстановлювати з'єднання Ethernet під час ініціювання бездротового зв'язку) Для запуску виявлення DHCP із пристрою, який знаходиться за мостом, міст перевстановлюватиме з'єднання Ethernet між мостом і пристроєм під час кожного встановлення бездротового зв'язку. Щоб вимкнути цю функцію, виберіть значення **No** (Ні). В іншому разі залиште значення за замовчуванням **Yes** (Так).

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Administration (Адміністрування) > Management (Керування)

На цьому екрані можна керувати особливими функціями моста: доступом до службової програми, що працює у браузері, резервним копіюванням файлу конфігурації, а також перезавантаженням.



Management (Керування)

Bridge Access (Доступ до моста)

Доступ до службової програми, що працює у браузері, можна захистити паролем.

Bridge Password (Пароль до моста) Введіть новий пароль для захисту доступу до моста.

Re-enter to confirm (Повторне введення) Введіть пароль ще раз, щоб підтвердити його.

Idle Timeout (Час очікування за відсутності дій) Тут можна задати тривалість очікування до виходу з системи за відсутності дій користувача. Діапазон значень: від **60** до **3600** секунд. Значення за замовчуванням: **600**.

Web Access (Веб-доступ)

Access via Wireless (Доступ із бездротової мережі) Якщо міст використовується у громадському місті, де доступ до бездротової мережі надається відвідувачам, можна заборонити доступ із бездротової мережі до службової програми моста, що працює у браузері. Якщо вимкнути цю можливість, доступ до службової програми моста буде можливий лише через дротове з'єднання. Залиште значення за замовчуванням **Enabled** (Увімкнено), щоб дозволити доступ до службової програми моста з бездротової мережі. Виберіть значення **Disabled** (Вимкнено), щоб заборонити доступ до службової програми з бездротової мережі.

Backup and Restore (Резервне копіювання та відновлення)

Backup (Резервне копіювання) Щоб створити резервну копію файлу конфігурації моста, виберіть **Backup Configurations** (Створити резервну копію конфігурації). Потім виконайте інструкції на екрані.

Restore (Відновлення) Натисніть кнопку **Browse** (Огляд) і виберіть файл конфігурації. Потім натисніть **Restore Configurations** (Відновити конфігурацію).

System Reboot (Перезавантаження системи)

Reboot (Перезавантаження) Щоб перезавантажити або перезапустити міст, натисніть **Start to Reboot** (Почати перезавантаження).

Натисніть **Save Settings** (Зберегти значення параметрів), щоб застосувати зміни, або **Cancel Changes** (Скасувати зміни), щоб скасувати зміни.

Administration (Адміністрування) > Factory Defaults (Заводські значення параметрів)

На цьому екрані можна відновити заводську конфігурацію моста.

Factory Defaults (Заводські значення параметрів)

Restore All Settings (Відновити значення всіх параметрів) Щоб відновити заводські значення параметрів моста, натисніть **Restore All Settings** (Відновити значення всіх параметрів). Під час відновлення заводських значень усі значення параметрів, збережені користувачем, будуть видалені.



Administration (Адміністрування) > Upgrade Firmware (Оновлення мікропрограмного забезпечення)

На цьому екрані можна оновити мікропрограмне забезпечення моста. Оновлюйте мікропрограмне забезпечення лише в разі, якщо виникають проблеми з використанням моста або якщо в новій версії мікропрограмного забезпечення з'явилася потрібна функція.



Перш ніж оновлювати мікропрограмне забезпечення, завантажте оновлення мікропрограмного забезпечення з веб-сайту Linksys **www.Linksys.com/support**.

Upgrade Firmware (Оновлення мікропрограмного забезпечення)

Please select a file to upgrade the firmware (Виберіть файл оновлення мікропрограмного забезпечення) Натисніть **Browse** (Огляд) і виберіть відповідний файл. Потім натисніть **Start to Upgrade** (Почати оновлення) та виконуйте інструкції на екрані.

Status (Стан) > Bridge (Міст)

Тут відображається інформація про поточний стан моста.



Bridge Information (Інформація про міст)

Firmware Version (Версія мікропрограмного забезпечення) Відображається поточна версія мікропрограмного забезпечення моста.

Local Network (Локальна мережа)

Local MAC Address (Локальна MAC-адреса) Відображається MAC-адреса моста, під якою він зареєстрований у локальній мережі Ethernet.

Local IP Address (Локальна IP-адреса) Відображається IP-адреса моста, під якою він зареєстрований у локальній мережі Ethernet.

Subnet Mask (Маска підмережі) Відображається значення маски підмережі, задане в локальній мережі.

Status (Стан) > Wireless (Бездротовий зв'язок)

Тут відображається інформація про бездротову мережу.



Wireless (Бездротовий зв'язок)

Link Status (Стан каналу) Відображається стан з'єднання з бездротовою мережею.

MAC Address (MAC-адреса) Відображається MAC-адреса моста, під якою він зареєстрований у локальній бездротовій мережі.

Network Name (SSID) (Ім'я мережі (SSID)) Відображається ім'я бездротової мережі (Ідентифікатор SSID).

BSSID Відображається MAC-адреса підключеного бездротового маршрутизатора (або точки доступу) в бездротовій мережі.

Radio Band (Діапазон радіочастот) Відображається діапазон радіочастот бездротової мережі.

Channel Width (Ширина каналу) Відображається ширина каналу (МГц), який використовується бездротовою мережею.

Wide Channel (Широкий канал) Залежно від значень параметрів каналу, заданих на мережевому маршрутизаторі, може відображатися широкий канал. Якщо для параметра радіочастоти або ширини каналу маршрутизатора вибрано значення широкого каналу 40 МГц, цей канал буде пріоритетним каналом бездротової мережі.

Standard Channel (Стандартний канал) Відображається значення стандартного каналу. Якщо для параметра радіочастоти або ширини каналу маршрутизатора вибрано значення широкого каналу 40 МГц, стандартний канал буде другорядним каналом бездротової мережі.

Bit Rate (Швидкість передавання даних) Відображається швидкість передавання даних.

Signal (Сигнал) Відображається рівень сигналу в процентах. Значення 100 % відповідає максимальному рівню сигналу; 0 % — мінімальному.

Security (Захист) Відображається метод захисту бездротової мережі.

Усунення несправностей

WES610N/WET610N

Комп'ютер або інший дротовий пристрій (зі з'єднанням Ethernet) не може обмінюватися даними із бездротовим маршрутизатором.

1. Відкрийте службову програму моста, що працює у браузері.
2. Перейдіть на екран *Basic Wireless Settings* (Базові налаштування бездротової мережі) та перевірте, чи відповідає значення параметра Network Name (SSID) (Ім'я мережі (SSID)) фактичному імені бездротової мережі.
3. Переконайтеся в тому, що значення параметра захисту (WPA, WPA2 або WEP) відповідає методу захисту бездротової мережі.

Необхідно змінити IP-адресу моста.

Якщо міст підключений до мережі із DHCP-сервером (зазвичай – мережевим маршрутизатором), міст отримує IP-адресу від DHCP-сервера. Якщо DHCP-сервер відсутній, міст використовуватиме статичну IP-адресу за замовчуванням: **169.254.1.250**.

Щоб надати мосту постійну статичну IP-адресу, виконайте наведені нижче інструкції.

1. Відкрийте службову програму моста, що працює у браузері.
2. Виберіть вкладку **Network Setup** (Налаштування мережі).
3. Із розкривного меню *Network Connection Type* (Тип мережевого з'єднання) виберіть **Static IP** (Статична IP-адреса).
4. Заповніть поля *Static IP Address* (Статична IP-адреса), *Subnet Mask* (Маска підмережі) та *Default Gateway* (Шлюз за замовчуванням).
5. Натисніть кнопку **Save Settings** (Зберегти значення параметрів).

Комп'ютер або інший дротовий пристрій (зі з'єднанням Ethernet), підключений до мосту, не обмінюється даними з іншим пристроєм (наприклад, комп'ютером або принтером), підключеним до бездротової мережі.

Перевірте зазначені нижче умови.

- Переконайтеся в тому, що пристрій, підключений до бездротової мережі, належить до тієї самої мережі, що й комп'ютер або інший дротовий пристрій (зі з'єднанням Ethernet), підключений до мосту.
- Перевірте, чи використовується на всіх пристроях, підключених до бездротової мережі, те саме ім'я мережі (SSID).
- Переконайтеся в тому, що всі пристрої належать до тієї самої IP-мережі та мають сумісні IP-адреси.

Службова програма, що працює у браузері, не приймає пароль.

Перевірте зазначені нижче умови.

- Пароль чутливий до регістру. Ураховуйте регістр символів під час введення пароля.
- Якщо пароль забуто, можна відновити заводські значення параметрів моста.

 Натисніть і утримуйте близько п'яти секунд кнопку **Reset** (Скидання) на мості. Буде відновлено пароль за замовчуванням **admin**. Буде також відновлено заводські значення всіх інших параметрів. (Щоб увійти до службової програми, що працює у браузері, введіть **admin** у поле *Password* (Пароль).)

Після внесення змін за допомогою службової програми, що працює у браузері, нові значення параметрів не відображаються на екрані.

Виконайте функцію **Оновити** у веб-браузері. Якщо нові значення параметрів все одно не відображаються, виконайте наведені нижче інструкції.

1. Від'єднайте адаптер живлення від моста.
2. Зачекайте п'ять секунд, а потім знову приєднайте адаптер живлення до моста.
3. Виконайте функцію **Оновити** у веб-браузері.

ВЕБ-ПІДТРИМКА
Якщо не вдалося знайти відповіді на питання у цьому посібнику, відвідайте веб-сайт Linksys за адресою **Linksys.com/support**

Технічні характеристики

WES610N

Модель	WES610N
Стандарти	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Світлодіодні індикатори	Живлення, Ethernet, Wi-Fi Protected Setup™, Бездротовий зв'язок, окремий індикатор каналу Ethernet і його активності
Порти	Ethernet (4 шт.), Живлення
Кнопки	Reset (Скидання), Wi-Fi Protected Setup
Тип кабельного з'єднання	CAT5e
Антени	3 (внутрішні)
Тип з'єднання антени	дані відсутні
Знімне виконання (так/ні)	ні
Модуляції	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Рівень радіочастотного сигналу (EIRP) у дБм	802.11a: 15 дБм (типовий) за 54 Мбіт/с 802.11b: 19 дБм (типовий) за 11 Мбіт/с 802.11g: 16 дБм (типовий) за 54 Мбіт/с 802.11n (2,4 ГГц): 18 дБм (типовий) за MCS15 802.11n (5 ГГц): 16 дБм (типовий) за MCS15
Рівень чутливості прийому	802.11a: –72 дБм (типовий) за 54 Мбіт/с 802.11b: –85 дБм (типовий) за 11 Мбіт/с 802.11g: –73 дБм (типовий) за 54 Мбіт/с 802.11n (20 ГГц): –75 дБм (типовий) за MCS15 802.11n (40 ГГц): –69 дБм (типовий) за MCS15
Підсилення антени, дБі	1
Захист бездротового зв'язку	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Розряд ключа захисту	до 128-розрядного шифрування

Зовнішні чинники

Розміри	6,97 x 5,04 x 2,68 дюйма (177 x 128 x 68 мм
Вага	0,65 фунта (295 г)
Сертифікація	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/проект n), WPA2™, Wi-Fi Protected Setup, WMM®
Живлення	12 В, 1 А
Робоча температура	32—104 °F (0—40 °C)
Температура під час зберігання	від –4 до 140 °F (від –20 до 60 °C)
Робоча вологість	10—85 %, без конденсації
Вологість під час зберігання	5—90 %, без конденсації

Технічні характеристики можуть бути змінені без попередження.

WET610N

Модель	WET610N
Стандарти	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Світлодіодні індикатори	Живлення, Ethernet, Wi-Fi Protected Setup™, Бездротовий зв'язок
Порти	Ethernet, Живлення
Кнопки	Reset (Скидання), Wi-Fi Protected Setup
Тип кабельного з'єднання	CAT5e
Антени	3 (внутрішні)
Тип з'єднання антени	дані відсутні
Знімне виконання (так/ні)	ні
Модуляції	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Рівень радіочастотного сигналу (EIRP) у дБм	802.11a: 15 дБм (типовий) за 54 Мбіт/с 802.11b: 18 дБм (типовий) за 11 Мбіт/с 802.11g: 16 дБм (типовий) за 54 Мбіт/с 802.11n: 12 дБм (типовий) за 130 Мбіт/с (HT20), 270 Мбіт/с (HT40)
Рівень чутливості прийому	802.11a: –72 дБм (типовий) за 54 Мбіт/с 802.11b: –85 дБм (типовий) за 11 Мбіт/с 802.11g: –73 дБм (типовий) за 54 Мбіт/с 802.11n: –70 дБм (типовий) за MCS15/2,4 ГГц, –69 дБм (типовий) за MCS15/5,0 ГГц
Підсилення антени, дБі	1
Захист бездротового зв'язку	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Розряд ключа захисту	до 128-розрядного шифрування

Зовнішні чинники

Розміри	5,71 x 4,17 x 2,05 дюйма (145 x 106 x 52 мм)
Вага	5,61 унції (159 г)
Сертифікація	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/проект n), WPA2™, Wi-Fi Protected Setup, WMM®
Живлення	12 В, 1 А
Робоча температура	32—104 °F (0—40 °C)
Температура під час зберігання	від –4 до 140 °F (від –20 до 60 °C)
Робоча вологість	10—85 %, без конденсації
Вологість під час зберігання	5—90 %, без конденсації

Технічні характеристики можуть бути змінені без попередження.

Linksys.com/support

Cisco, логотип Cisco та Linksys є торговими марками або зареєстрованими торговими марками компанії Cisco та/або її дочірніх компаній у США та інших країнах.
Список торгових марок Cisco можна знайти за адресою www.cisco.com/go/trademarks. Усі інші торгові марки, згадані в цьому документі, належать відповідним власникам.

© 2011 р. Компанія Cisco та/або її дочірні компанії. Усі права захищено.

3425-01249



Hướng dẫn Sử dụng

Linksys WET610N/WES610N | Cầu nối Giải trí chuẩn N Dải kép

Mục lục

Tổng quan Sản phẩm

Mặt bố trí đèn LED 2
Mặt bố trí các cổng 3

Danh sách kiểm tra Bảo mật Không dây

Thay đổi tên mạng không dây hoặc SSID mặc định 4
Thay đổi mật khẩu mặc định 4
Bật tính năng lọc địa chỉ MAC 4
Bật mã hóa 4

Hướng dẫn Chung về Bảo mật Mạng 4
Mẹo Bảo mật Bổ sung 5

Cấu hình nâng cao

Cách truy cập tiện ích dựa trên trình duyệt 6
Setup (Cài đặt) > Basic Setup (Cài đặt Cơ bản) 7
Language (Ngôn ngữ) 7
Network Setup (Cài đặt Mạng) 7
Wireless (Không dây) > Basic Wireless Settings (Cài đặt không dây cơ bản) 7
Basic Wireless Settings (Cài đặt không dây cơ bản) 8
Wireless Security (Bảo mật không dây) 8
Wi-Fi Protected Setup (Thiết lập Bảo mật WiFi) 9
Wireless (Không dây) > Wireless Network Site Survey (Quét Khu vực Mạng Không dây) 10
Wireless Network Site Survey (Quét Khu vực Mạng Không dây) 10
Wireless (Không dây) > WMM® 11
WMM 12
Wireless (Không dây) > Advanced Wireless Settings (Cài đặt Không dây Nâng cao) 13
Advanced Wireless (Không dây Nâng cao) 14
Administration (Quản trị) > Management (Quản lý) 14
Management (Quản lý) 14
Administration (Quản trị) > Factory Defaults (Giá trị Mặc định khi Xuất xưởng) 15
Factory Defaults (Giá trị Mặc định khi Xuất xưởng) 15
Administration (Quản trị) > Upgrade Firmware (Nâng cấp Phần mềm Hệ thống) 15
Upgrade Firmware (Nâng cấp Phần mềm Hệ thống) 16
Status (Trạng thái) > Bridge (Cầu nối) 16
Bridge Information (Thông tin về Cầu nối) 16
Local Network (Mạng Nội bộ) 16
Status (Trạng thái) > Wireless (Không dây) 16
Wireless (Không dây) 16

Khắc phục sự cố

WES610N/WET610N 17

Thông số kỹ thuật

WES610N 18
WET610N 19

Tổng quan Sản phẩm

Cám ơn bạn đã chọn mua thiết bị Cầu nối Giải trí chuẩn N dải kép của Linksys. Cầu nối này có thể kết nối bất kỳ thiết bị có dây, Ethernet nào với mạng không dây của bạn. Cầu nối dựa trên chuẩn Wireless-N dải kép, vì vậy cầu nối này tương thích với bất kỳ điểm truy cập hay bộ định tuyến chuẩn Wireless-N, -G, -A, hoặc -B nào. Hãy làm theo các bước trong thư mục CD cho lần cài đặt đầu tiên. Để cấu hình cài đặt nâng cao, hãy sử dụng tiện ích tiện dụng, dựa trên trình duyệt.

Mặt bố trí đèn LED



WES610N WET610N

Không dây (Xanh) Đèn LED Không dây bật sáng khi có kết nối không dây. Đèn LED nháy sáng khi cầu nối đang gửi hay nhận dữ liệu qua mạng không dây.

Nút Wi-Fi Protected Setup Nếu bộ định tuyến của bạn hỗ trợ Wi-Fi Protected Setup và sử dụng tính năng bảo mật WPA hay WPA2, bạn có thể sử dụng Wi-Fi Protected Setup để tự động kết nối với cầu nối. Để sử dụng Wi-Fi Protected Setup (Thiết lập bảo mật WiFi), tham khảo "Wireless (Không dây) > Basic Wireless Settings (Cài đặt không dây cơ bản)" trên trang 7.

Đèn LED Wi-Fi Protected Setup (Xanh/Hổ phách) Đèn LED nháy sáng màu xanh trong hai phút trong khi sử dụng Wi-Fi Protected Setup. Đèn này sẽ bật sáng màu xanh khi thiết bị có bật tính năng bảo mật không dây. Nếu xảy ra lỗi trong khi sử dụng Wi-Fi Protected Setup, Đèn LED sẽ bật sáng sang màu hổ phách. Hãy đảm bảo bộ định tuyến mạng có hỗ trợ Wi-Fi Protected Setup. Đợi cho đến khi đèn LED tắt, rồi thử lại lần nữa.

Ethernet (Xanh) Đèn LED Ethernet bật sáng khi có kết nối có dây. Đèn LED nháy sáng khi cầu nối đang gửi hay nhận dữ liệu qua (các) cổng Ethernet.

Nguồn (Xanh) Đèn Nguồn bật sáng khi cầu nối được bật nguồn.

Mặt bố trí các cổng



WES610N WET610N

Ethernet Cổng Ethernet kết nối cầu nối với một máy tính hoặc qua thiết bị mạng Ethernet khác. WES610N có bốn cổng còn WET610N có một cổng.

Nút Reset (Cài lại) Có hai cách để cài lại giá trị mặc định khi xuất xưởng của cầu nối. Bấm và giữ nút Reset (Cài lại) khoảng 5 giây hoặc khôi phục lại giá trị mặc định từ Administration (Quản trị) > Factory Defaults (Giá trị mặc định khi xuất xưởng) trong tiện ích dựa trên trình duyệt của cầu nối. WES610N có nút cài lại ở mặt đáy còn WET610N có nút cài lại ở mặt bố trí các cổng ở phía sau.

Nguồn Cổng nguồn kết nối cầu nối với bộ thích ứng nguồn đi kèm.

Danh sách kiểm tra Bảo mật Không dây

Các mạng không dây khá thuận tiện và dễ cài đặt vì vậy số hộ gia đình có truy cập internet tốc độ cao sử dụng mạng không dây đang tăng lên khá nhanh. Do kết nối mạng không dây hoạt động bằng cách gửi thông tin qua sóng vô tuyến, nó có thể dễ bị những kẻ xâm phạm tấn công hơn so với mạng có dây truyền thống. Giống như tín hiệu từ điện thoại di động hoặc điện thoại có dây, các tín hiệu từ mạng không dây của bạn cũng có thể bị chặn lại. Do bạn không thể ngăn ai đó kết nối vào mạng không dây của mình, bạn cần thực hiện thêm một số bước nhằm giữ cho mạng của bạn an toàn.

Thay đổi tên mạng không dây hoặc SSID mặc định

Các thiết bị không dây có một tên mạng không dây mặc định hoặc Mã định danh Thiết đặt Dịch vụ (SSID) do nhà máy sản xuất thiết bị cài đặt. Đây là tên mạng không dây của bạn và nó có thể dài tới 32 ký tự. Các sản phẩm không dây của Linksys dùng **linksys** là tên mạng không dây mặc định Bạn nên thay đổi tên mạng không dây thành một tên gì đó độc đáo để phân biệt mạng không dây của mình với các mạng không dây khác có thể tồn tại xung quanh bạn nhưng không sử dụng thông tin cá nhân (chẳng hạn như số bảo hiểm xã hội của bạn) vì bất kỳ ai cũng có thể nhìn thấy thông tin này khi duyệt các mạng không dây.

Thay đổi mật khẩu mặc định

Đối với các sản phẩm không dây như bộ định tuyến hay điểm truy cập, bạn sẽ được yêu cầu cung cấp mật khẩu khi muốn thay đổi cài đặt của thiết bị. Những thiết bị này có mật khẩu mặc định được nhà máy sản xuất thiết bị cài đặt. Mật khẩu mặc định của Linksys là **admin**. Tin tặc biết các mật khẩu mặc định này và có thể cố gắng sử dụng chúng để truy cập vào thiết bị không dây của bạn và thay đổi cài đặt mạng của bạn. Để ngăn chặn bất kỳ sự thay đổi trái phép nào, hãy tùy chỉnh mật khẩu của thiết bị sao cho nó trở nên khó đoán.

Bật tính năng lọc địa chỉ MAC

Các bộ định tuyến của Linksys cung cấp cho bạn khả năng bật tính năng lọc địa chỉ Kiểm soát Truy cập Phương tiện (MAC). Địa chỉ MAC là một dãy số và chữ duy nhất được gán cho mọi thiết bị kết nối mạng. Với tính năng lọc địa chỉ MAC được bật, quyền truy cập mạng không dây chỉ được cung cấp cho các thiết bị không dây có các địa chỉ MAC cụ thể. Ví dụ, bạn có thể chỉ định địa chỉ MAC cho từng máy tính trong gia đình bạn để chỉ những máy tính đó mới có thể truy cập mạng không dây của bạn.

Bật mã hóa

Mã hõa giúp bảo vệ dữ liệu được truyền qua mạng không dây. Wi-Fi Protected Access (WPA/WPA2) (Truy cập Wi-Fi được bảo vệ) và Wired Equivalent Privacy (WEP) (Bảo mật Tương đương có dây) cung cấp các cấp độ bảo mật khác nhau dành cho việc giao tiếp không dây.

Một mạng được mã hóa bằng chuẩn WPA/WPA2 sẽ an toàn hơn mạng được mã hóa bằng chuẩn WEP, vì WPA/WPA2 sử dụng mã hóa khóa động. Để bảo vệ thông tin khi những thông tin này được truyền qua sóng radio, bạn nên bật mức bảo mật cao nhất mà thiết bị mạng của bạn hỗ trợ.

WEP là chuẩn mã hóa cũ hơn và có thể là tùy chọn duy nhất sẵn có trên các thiết bị đời trước không hỗ trợ chuẩn WPA.

Hướng dẫn Chung về Bảo mật Mạng

Bảo mật mạng không dây sẽ không có giá trị nếu mạng cơ sở không an toàn.

- Mật khẩu bảo vệ tất cả các máy tính trên mạng và mật khẩu cá nhân bảo vệ các tệp nhạy cảm.
- Thường xuyên thay đổi mật khẩu.
- Cài đặt phần mềm chống vi-rút và các phần mềm tường lửa cá nhân.
- Tắt chia sẻ tệp (ngang hàng). Một số ứng dụng có thể mở tính năng chia sẻ tệp mà bạn không biết và/hoặc không được sự đồng ý của bạn.

Mẹo Bảo mật Bổ sung

- Giữ bộ định tuyến không dây, các điểm truy cập hay các cổng cánh xa các bức tường và cửa sổ bên ngoài.
- Tắt bộ định tuyến, các điểm truy cập hay các cổng khi không sử dụng chúng (vào ban đêm, trong các kỳ nghỉ).
- Sử dụng các mật mã mạnh có ít nhất 8 ký tự. Kết hợp cả chữ và số nhằm tránh dùng các từ chuẩn có thể tìm thấy trong từ điển.

Cấu hình nâng cao

Sau khi cài đặt cầu nối bằng cách làm theo các bước trong thư mục CD, cầu nối sẽ sẵn sàng để sử dụng. Tuy nhiên, nếu bạn muốn thay đổi cài đặt nâng cao của cầu nối, hãy sử dụng tiện ích dựa trên trình duyệt của cầu nối. Chương này mô tả từng trang web của tiện ích và các chức năng chính của mỗi trang. Bạn có thể truy cập tiện ích qua một trình duyệt web trên máy tính có nối mạng với cầu nối.

Tiện ích dựa trên trình duyệt có những tab chính: Setup (Thiết lập), Wireless (Không dây), Administration (Quản trị) và Status (Trạng thái). Các tab bổ sung sẽ sẵn có sau khi bạn nhấp vào một tab chính.

Cách truy cập tiện ích dựa trên trình duyệt

Sử dụng một trình duyệt web để truy cập tiện ích dựa trên trình duyệt.

Nếu cầu nối được nối với mạng bằng máy chủ DHCP (thường là bộ định tuyến mạng), cầu nối sẽ nhận địa chỉ IP của mình từ máy chủ DHCP. Nếu không có máy chủ DHCP, cầu nối sẽ sử dụng địa chỉ IP tĩnh, mặc định là **169.254.1.250**. (Nếu bạn cài một địa chỉ IP tĩnh thường xuyên trên cầu nối qua tiện ích dựa trên trình duyệt, hãy nhập địa chỉ IP tĩnh)

> **LƯU Ý**
> Nếu bạn không biết địa chỉ IP của cầu nối, hãy tìm địa chỉ IP trong bảng máy khách DHCP của bộ định tuyến. (Tham khảo tài liệu dành cho bộ định tuyến của bạn)
>
> Nếu bạn không thể tìm thấy địa chỉ IP của cầu nối, bạn có thể cài lại cầu nối; bấm nút **Reset** (Cài lại) trên cầu nối khoảng 5 giây, bằng cách sử dụng một ghim kẹp giấy thẳng. Thao tác này sẽ cài lại cầu nối trở về cài đặt mặc định khi xuất xưởng. Cầu nối sẽ yêu cầu địa chỉ IP từ máy chủ DHCP (thường là bộ định tuyến mạng). Nếu không tìm thấy máy chủ DHCP, cầu nối sẽ sử dụng địa chỉ IP tĩnh mặc định của nó, **169.254.1.250**, cho đến khi cầu nối phát hiện được một máy chủ DHCP và được gán một địa chỉ IP động.

Nếu cầu nối không được kết hợp với một bộ định tuyến và sử dụng cài đặt mặc định khi xuất xưởng, hãy kết nối máy tính với cầu nối bằng kết nối Ethernet để truy cập tiện ích dựa trên- trình duyệt. Bạn sẽ cần cấu hình kết nối Ethernet trên máy tính với địa chỉ IP tĩnh và mặt nạ mạng phụ.

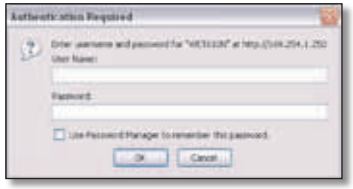
Địa chỉ IP của bộ thích ứng Ethernet của bạn phải được cài một địa chỉ IP cụ thể.

1. Trong trường *IP address* (Địa chỉ IP), hãy nhập **169.254.x.y** (x sẽ là một số trong khoảng từ 1 đến 254 và y sẽ là một số trong khoảng từ 0 đến 255).
2. Trong trường *Subnet mask* (Mặt nạ mạng phụ), hãy nhập **255.255.0.0**.

> **LƯU Ý**
> Các bước để gán địa chỉ IP tĩnh cho bộ thích ứng Ethernet trên máy tính của bạn thay đổi tùy thuộc vào hệ điều hành. Để có hướng dẫn, vui lòng tham khảo tài liệu trợ giúp của hệ điều hành cụ thể của bạn.

Sau khi gán địa chỉ IP tĩnh cho bộ thích ứng Ethernet, hãy khởi chạy trình duyệt web và nhập địa chỉ IP của Bộ thích ứng (cài đặt mặc định là **169.254.1.250**) trong trường *Address* (Địa chỉ). Bấm **Enter**.

Màn hình yêu cầu mật khẩu xuất hiện. (Người dùng không sử dụng Windows XP sẽ nhìn thấy một màn hình tương tự.) Để trống trường *User name* (Tên người dùng). Nhập mật khẩu bạn đã tạo trong quá trình thực hiện Thuật sĩ Cài đặt. Nếu bạn chưa tạo mật khẩu mới, hãy sử dụng mật khẩu mặc định **admin**. (Bạn có thể cài mật khẩu mới từ màn hình *Administration* (Quản trị) > *Management* (Quản lý).) Nhấp **OK** để tiếp tục.



> **LƯU Ý**
> Nếu màn hình yêu cầu mật khẩu không xuất hiện, hãy đợi 2 phút rồi thử lại.

Setup (Cài đặt) > Basic Setup (Cài đặt Cơ bản)

Màn hình đầu tiên xuất hiện là màn hình *Basic Setup* (Cài đặt Cơ bản). Sử dụng màn hình này để thay đổi ngôn ngữ của tiện ích dựa trên trình duyệt, hoặc để thay đổi cài đặt mạng Ethernet có dây của cầu nối.





Language (Ngôn ngữ)

Language (Ngôn ngữ) Mục này được dùng để cài ngôn ngữ mà tiện ích dựa trên trình duyệt hiển thị. Chọn ngôn ngữ mong muốn từ menu thả xuống.

Network Setup (Cài đặt Mạng)

Mục này xác định liệu địa chỉ IP của cầu nối được nhận tự động từ một máy chủ DHCP không, chẳng hạn như bộ định tuyến mạng của bạn (Automatic Configuration - DHCP) (Cấu hình Tự động - DHCP), hay được cài đặt thủ công (Static IP) (IP Tĩnh).

Bridge IP (IP Cầu nối) Nếu mạng của bạn có một máy chủ DHCP, chẳng hạn như bộ định tuyến mạng, gán các địa chỉ IP cho các thiết bị mạng của bạn thì hãy giữ nguyên giá trị mặc định **Automatic Configuration - DHCP** (Cấu hình Tự động - DHCP). Cầu nối sẽ yêu cầu địa chỉ IP từ máy chủ DHCP (thường là bộ định tuyến mạng). Nếu không tìm thấy máy chủ DHCP, cầu nối sẽ sử dụng địa chỉ IP tĩnh mặc định của nó, **169.254.1.250**,cho đến khi cầu nối phát hiện được một máy chủ DHCP và được gán một địa chỉ IP động.

Nếu bạn muốn cài một địa chỉ IP tĩnh thường xuyên cho cầu nối, hãy chọn **Static IP** (IP Tĩnh).

Nếu bạn chọn Static IP, hãy điền các trường sau

- **Static IP Address** (Địa chỉ IP Tĩnh) Nhập một địa chỉ IP duy nhất sẽ được sử dụng để truy cập tiện ích dựa trên trình duyệt
- **Subnet Mask** (Mặt nạ Mạng phụ) Nhập mặt nạ mạng phụ cho mạng có dây của bạn.
- **Default Gateway** (Cổng Mặc định) Nhập địa chỉ IP của cổng mặc định cho mạng của bạn (trong hầu hết các trường hợp, đây là bộ định tuyến của bạn).

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Wireless (Không dây) > Basic Wireless Settings (Cài đặt không dây cơ bản)

Sử dụng màn hình *Basic Wireless Settings* (Cài đặt không dây cơ bản) để cấu hình cài đặt bảo mật và không dây cơ bản của cầu nối.

Có hai cách để cấu hình cài đặt của cầu nối, thủ công và Wi-Fi Protected Setup (Thiết lập Bảo mật Wi-Fi). Wi-Fi Protected Setup (Thiết lập bảo mật Wi-Fi) là một tính năng giúp bạn dễ dàng cài đặt mạng không dây của mình. Nếu bộ định tuyến của bạn hỗ trợ Wi-Fi Protected Setup và sử dụng tính năng bảo mật WPA hay WPA2, bạn có thể sử dụng Wi-Fi Protected Setup để tự động kết nối với cầu nối.

Configuration View (Giao diện Cấu hình) Để cấu hình thủ công mạng không dây của bạn, chọn **Manual** (Thủ công). Tham khảo phần **Basic Wireless Settings** (Cài đặt không dây cơ bản), **trang 8**. Để sử dụng Wi-Fi Protected Setup, chọn **Wi-Fi Protected Setup** (Thiết lập Bảo mật Wi-Fi). Tham khảo phần **Wi-Fi Protected Setup** (Thiết lập Bảo mật WiFi), **trang 9**.

Basic Wireless Settings (Cài đặt không dây cơ bản)



Network Name (SSID) (Tên mạng) SSID là tên mạng mà tất cả các thiết bị trong mạng không dây dùng chung. SSID phải giống nhau cho tất cả các thiết bị trong mạng không dây. Tên mạng có phân biệt kiểu chữ và không được vượt quá 32 ký tự (sử dụng bất kỳ ký tự nào có trên bàn phím). Đảm bảo cài đặt này khớp với cài đặt trên bộ định tuyến không dây hoặc điểm truy cập của bạn. Để được bảo mật thêm, bạn nên thay đổi SSID (**linksys**) thành một tên độc đáo.

Wireless Security (Bảo mật không dây)

Cầu nối hỗ trợ các tuỳ chọn bảo mật không dây sau: WPA Personal (WPA Cá nhân), WPA2 Personal (WPA2 Cá nhân) và WEP. WPA (Wi-Fi Protected Access - (Truy cập Wi-Fi được bảo vệ)) và WPA2 là các phương thức bảo mật mạnh hơn WEP (Wired Equivalent Privacy - (Bảo mật Tương đương có dây)). Để có thêm thông tin về bảo mật không đây, tham khảo phần "Danh sách kiểm tra Bảo mật Không dây", trang 4.

Security Mode (Chế độ Bảo mật)

Chọn phương thức bảo mật cho mạng không dây của bạn. Nếu bạn không muốn dùng bảo mật không dây, giữ nguyên giá trị mặc định, **Disabled** (Tắt).

LƯU Ý
Hãy nhớ rằng mỗi thiết bị trong mạng không dây của bạn PHẢI sử dụng cùng một phương thức bảo mật, mật mã/mã khóa, nếu không các thiết bị không dây sẽ không thể giao tiếp với nhau.

WPA Cá nhân

WPA là chuẩn bảo mật mạnh hơn tính năng mã hóa WEP.



Encryption (Mã hóa) WPA hỗ trợ phương thức mã hóa TKIP với các mã khóa mã hóa động.

Passphrase (Mật mã) Nhập mã khóa được dùng chung cho cả cầu nối, bộ định tuyến không dây và điểm truy cập của bạn. Mã khóa phải từ 8 đến 63 ký tự.

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

WPA2 Cá nhân

WPA2 là phiên bản nâng cao hơn và an toàn hơn của WPA.



Encryption (Mã hóa) WPA2 hỗ trợ hai phương thức mã hóa, TKIP và AES, với các mã khóa mã hóa động. Chọn phương thức mã hóa, **AES or TKIP** (AES hoặc TKIP) hoặc **AES**. Lựa chọn mặc định là **AES**.

Passphrase (Mật mã) Nhập mã khóa được dùng chung cho cả cầu nối, bộ định tuyến không dây và điểm truy cập. Mã khóa phải từ 8 đến 63 ký tự.

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

WEP

WEP là phương thức mã hoá cơ bản, không an toàn bằng phương thức WPA hoặc WPA2.



Mã hóa Chọn cấp độ mã hoá WEP, **40/64 bits (10 hex digits)** (10 chữ số theo hệ hex 40/64-bit) hoặc **104/128 bits (26 hex digits)** (26 chữ số theo hệ hex 104/128bit). Mặc định là **40/64 bits (10 hex digits)** (10 chữ số theo hệ hex 40/64-bit).

Key 1 (Mã khóa 1) Nhập mã khóa WEP mạng của bạn.

Tx Key (Mã khóa Tx) **Key 1** (Mã khóa 1) là mã khóa truyền được cầu nối sử dụng.

Authentication (Xác thực) Giá trị mặc định là **Auto** (Tự động) cho phép sử dụng xác thực hệ thống Open (Mở) hoặc mã khóa Shared (Dùng chung). Chọn **Open** (Mở) để sử dụng xác thực hệ thống mở, người gửi và người nhận không sử dụng mã khóa WEP để xác thực. Chọn **Shared** (Dùng chung) để sử dụng xác thực mã khóa được chia sẻ

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Wi-Fi Protected Setup (Thiết lập Bảo mật WiFi)

Hiện có sẵn hai phương thức Sử dụng phương thức áp dụng cho bộ định tuyến mà bạn đang dùng.





Phương thức #1

Sử dụng phương thức này nếu bộ định tuyến của bạn có nút Wi-Fi Protected Setup (Thiết lập Bảo mật WiFi).

1. Bấm hoặc nhấp nút **Wi-Fi Protected Setup** (Thiết lập Bảo mật WiFi) trên bộ định tuyến.
2. Trong vòng hai phút, nhấp nút **Wi-Fi Protected Setup** (Thiết lập Bảo mật WiFi) trên màn hình *Wi-Fi Protected Setup* (Thiết lập Bảo mật WiFi).
3. Sau khi đã hoàn tất cấu hình cầu nối, nhấp **Close** (Đóng).

Màn hình *Wi-Fi Protected Setup* (Thiết lập Bảo mật WiFi) hiển thị phương thức bảo mật, Link Status (Trạng thái Liên kết) và Network Name (SSID) (Tên Mạng).

Phương thức #2

Sử dụng phương thức này nếu bộ định tuyến của bạn yêu cầu mã số PIN của cầu nối.

1. Trên màn hình *Wi-Fi Protected Setup* (Thiết lập Bảo mật WiFi) của **bộ định tuyến**, hãy nhập mã số PIN trên màn hình*Wi-Fi Protected Setup* (Thiết lập Bảo mật WiFi) của **cầu nối**. Sau đó nhấp **Register** (Đăng ký) hoặc nút tương ứng. (PIN này cũng được ghi ở mặt dưới của cầu nối).
2. Trên màn hình *Wi-Fi Protected Setup* (Thiết lập Bảo mật WiFi) của **cầu nối**, hãy nhấp **OK**.
3. Sau khi đã hoàn tất cấu hình cầu nối, nhấp **Close** (Đóng).

Màn hình *Wi-Fi Protected Setup* (Thiết lập Bảo mật WiFi) hiển thị phương thức bảo mật, Link Status (Trạng thái Liên kết) và Network Name (SSID) (Tên Mạng).

Wireless (Không dây) > Wireless Network Site Survey (Quét Khu vực Mạng Không dây)

Nhấp vào tab **Wireless Network Site Survey** (Quét Khu vực Mạng Không dây) để bắt đầu quét khu vực. Màn hình *Wireless Network Site Survey* (Quét Khu vực Mạng Không dây) liệt kê các mạng không dây được cầu nối phát hiện thấy.



Wireless Network Site Survey (Quét Khu vực Mạng Không dây)

Number of Wireless Networks (Số Mạng Không dây) Hiển thị số mạng không dây được cầu nối phát hiện thấy.

Select (Chọn) Để kết nối với một mạng không dây, hãy nhấp **Select** (Chọn). Sau đó nhấp **Connect** (Kết nối).

Wireless Network Name (Tên Mạng Không dây) Hiển thị tên mạng hoặc SSID của mạng không dây.

GHz Hiển thị băng tần radio của mạng không dây.

Signal (Tín hiệu) Hiển thị tỉ lệ phần trăm cường độ tín hiệu. 100% là cường độ tín hiệu mạnh nhất có thể có; 0% là cường độ tín hiệu yếu nhất có thể có.

Security (Bảo mật) Nếu mạng hỗ trợ Wi-Fi Protected Setup, biểu tượng Wi-Fi Protected Setup sẽ hiển thị. Hiển thị phương thức bảo mật được mạng không dây sử dụng

Nhấp **Refresh** (Làm mới) để cập nhật thông tin trên màn hình.

Sau khi đã chọn mạng, hãy nhấp **Connect** (Kết nối). Một màn hình mới xuất hiện Làm theo các hướng dẫn dành cho phương thức bảo mật mạng của bạn

WPA



Network Name (SSID) (Tên Mạng) Tên mạng bạn chọn sẽ tự động được hiển thị

Security Mode (Chế độ Bảo mật) WPA Personal (WPA Cá nhân) sẽ tự động được hiển thị.

Encryption (Mã hóa) WPA hỗ trợ phương thức mã hóa TKIP với các mã khóa mã hóa động.

Passphrase (Mật mã) Nhập mã khóa được dùng chung cho cả cầu nối, bộ định tuyến không dây và điểm truy cập. Mã khóa phải từ 8 đến 63 ký tự.

Nhấp **Refresh** (Làm mới) để cập nhật thông tin trên màn hình.

Sau khi đã nhập cài đặt bảo mật, nhập **Connect** (Kết nối).

WPA2



Network Name (SSID) (Tên Mạng) Tên mạng bạn chọn sẽ tự động được hiển thị

Security Mode (Chế độ Bảo mật) WPA2 Personal (WPA2 Cá nhân) sẽ tự động được hiển thị.

Encryption (Mã hóa) WPA2 hỗ trợ hai phương thức mã hóa, TKIP và AES, với các mã khóa mã hóa động. Chọn phương thức mã hóa, **AES or TKIP** (AES hoặc TKIP) hoặc **AES**.

Passphrase (Mật mã) Nhập mã khóa được dùng chung cho cả cầu nối, bộ định tuyến không dây và điểm truy cập. Mã khóa phải từ 8 đến 63 ký tự.

Nhấp **Refresh** (Làm mới) để cập nhật thông tin trên màn hình.

Sau khi đã nhập cài đặt bảo mật, nhập **Connect** (Kết nối).

WEP



Network Name (SSID) (Tên Mạng) Tên mạng bạn chọn sẽ tự động được hiển thị

Security Mode (Chế độ Bảo mật) WEP sẽ tự động được hiển thị.

Mã hóa Chọn cấp độ mã hoá WEP, **40/64 bits (10 hex digits)** (10 chữ số theo hệ hex 40/64-bit) hoặc **104/128 bits (26 hex digits)** (26 chữ số theo hệ hex 104/128bit).

Key 1 (Mã khóa 1) Nhập mã khóa WEP mạng của bạn.

Tx Key (Mã khóa Tx) **Key 1** (Mã khóa 1) là mã khóa truyền được cầu nối sử dụng.

Authentication (Xác thực) Giá trị mặc định là **Auto** (Tự động) cho phép sử dụng xác thực hệ thống Open (Mở) hoặc mã khóa Shared (Dùng chung). Chọn **Open** (Mở) để sử dụng xác thực hệ thống mở, người gửi và người nhận không sử dụng mã khóa WEP để xác thực. Chọn **Shared** (Dùng chung) để sử dụng xác thực mã khóa được chia sẻ

Nhấp **Refresh** (Làm mới) để cập nhật thông tin trên màn hình.

Sau khi đã nhập cài đặt bảo mật, nhập **Connect** (Kết nối).

Wireless (Không dây) > WMM®

Cấu hình cài đặt Wireless MultiMedia (WMM) (Đa phương tiện Không dây). WMM ưu tiên các gói tin tùy thuộc vào chế độ truy cập tương ứng của chúng (loại lưu lượng): Background (Nền), Best Effort (Nỗ lực Tốt nhất), Video, hoặc Voice (Thoại). Các cài đặt này chỉ nên để một quản trị viên có chuyên môn điều chỉnh vì cài đặt không chính xác có thể làm giảm hiệu suất không dây.



LƯU Ý
Cài đặt trên màn hình *WMM* được thiết kế chỉ dành cho người dùng nâng cao.

WMM

Access Mode (Chế độ Truy cập)

Bạn có thể gán các cài đặt khác nhau cho bốn chế độ truy cập có sẵn. Chọn chế độ bạn muốn cấu hình **Background** (Nền), **Best Effort** (Nỗ lực Tốt nhất), **Video**, hoặc **Voice** (Thoại). Làm theo những hướng dẫn cho chế độ bạn chọn.

Background (Nền)

Use Aggregation (Sử dụng Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có thiết lập một phiên Thêm Xác nhận theo Khối (ADDBA). Giá trị mặc định là **No** (Không). Chọn **Yes** (Có) để bật tùy chọn này.

Accept Aggregation (Chấp nhận Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có chấp nhận yêu cầu ADDBA không. Mặc định là **Yes** (Có). Chọn **No** (Không) để tắt tùy chọn này.

Max. Number of Packets in Aggregation (Số Gói tin Tối đa trong Tập hợp) Tùy chọn này xác định số gói tin tối đa (khung phụ) trong tập hợp. Phạm vi từ **0** đến **7**. Mặc định là **7**.

Max. Aggregation Size (Kích cỡ Tối đa của Tập hợp) Tùy chọn này xác định kích cỡ tối đa của tập hợp (the byte). Phạm vi từ **0** đến **16000**. Mặc định là **12000**.

Timeout Internal (Thời gian chờ Nội bộ) Tùy chọn này xác định khoảng thời gian chờ theo đó tập hợp sẽ được đóng với "điều kiện đóng" trước khi bộ bấm giờ đóng tập hợp. Phạm vi từ **0** đến **100** ms. Mặc định là **3**.

Min. Size of Packet in Aggregation (Kích cỡ Tối thiểu của Gói tin trong Tập hợp) Tùy chọn này xác định kích cỡ tối thiểu của các gói tin được tích lũy trong tập hợp (the byte). Phạm vi từ **0** đến **1500**. Mặc định là **10**.

ADDBA Timeout (Thời gian chờ ADDBA) Tùy chọn này xác định khoảng thời gian sau đó cài đặt ADDBA sẽ chấm dứt, nếu không có trao đổi khung trong khoảng thời gian này theo thỏa thuận Xác nhận Khối (ACK). Phạm vi từ **0** đến **65535** ms. Giá trị mặc định là **0**, đây là giá trị tắt tính năng thời gian chờ .

Aggregation Window Size (Kích cỡ Cửa sổ Tập hợp) Tùy chọn này xác định số gói tin tối đa được truyền mà không cần nhận ACK. Phạm vi từ **0** đến **64**. Mặc định là **64**.

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Best Effort (Nỗ lực Tốt nhất)

Use Aggregation (Sử dụng Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có thiết lập một phiên Thêm Xác nhận theo Khối (ADDBA). Mặc định là **Yes** (Có). Chọn **No** (Không) để tắt tùy chọn này.

Accept Aggregation (Chấp nhận Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có chấp nhận yêu cầu ADDBA. Mặc định là **Yes** (Có). Chọn **No** (Không) để tắt tùy chọn này.

Max. Number of Packets in Aggregation (Số Gói tin Tối đa trong Tập hợp) Tùy chọn này xác định số gói tin tối đa (khung phụ) trong tập hợp. Phạm vi từ **0** đến **10**. Mặc định là **10**.

Max. Aggregation Size (Kích cỡ Tối đa của Tập hợp) Tùy chọn này xác định kích cỡ tối đa của tập hợp (the byte). Phạm vi từ **0** đến **20000**. Mặc định là **16000**.

Timeout Internal (Thời gia chờ Nội bộ) Tùy chọn này xác định khoảng thời gian chờ theo đó tập hợp sẽ được đóng với "điều kiện đóng" trước khi bộ bấm giờ đóng tập hợp. Phạm vi từ **0** đến **100** ms. Mặc định là **3**.

Min. Size of Packet in Aggregation (Kích cỡ Tối thiểu của Gói tin trong Tập hợp) Tùy chọn này xác định kích cỡ tối thiểu của các gói tin được tích lũy trong tập hợp (the byte). Phạm vi từ **0** đến **1500**. Mặc định là **10**.

ADDBA Timeout (Thời gian chờ ADDBA) Tùy chọn này xác định khoảng thời gian sau đó cài đặt ADDBA sẽ chấm dứt, nếu không có trao đổi khung trong khoảng thời gian này theo thỏa thuận Xác nhận Khối (ACK). Phạm vi từ **0** đến **65535** ms. Giá trị mặc định là **0**, đây là giá trị tắt tính năng thời gian chờ .

Aggregation Window Size (Kích cỡ Cửa sổ Tập hợp) Tùy chọn này xác định số gói tin tối đa được truyền mà không cần nhận ACK. Phạm vi từ **0** đến **64**. Mặc định là **64**.

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Video

Use Aggregation (Sử dụng Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có thiết lập một phiên Thêm Xác nhận theo Khối (ADDBA). Mặc định là **Yes** (Có). Chọn **No** (Không) để tắt tùy chọn này.

Accept Aggregation (Chấp nhận Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có chấp nhận yêu cầu ADDBA. Mặc định là **Yes** (Có). Chọn **No** (Không) để tắt tùy chọn này.

Max. Number of Packets in Aggregation (Số Gói tin Tối đa trong Tập hợp) Tùy chọn này xác định số gói tin tối đa (khung phụ) trong tập hợp. Phạm vi từ **0** đến **7**. Mặc định là **7**.

Max. Aggregation Size (Kích cỡ Tối đa của Tập hợp) Tùy chọn này xác định kích cỡ tối đa của tập hợp (the byte). Phạm vi từ **0** đến **16000**. Mặc định là **12000**.

Timeout Internal (Thời gia chờ Nội bộ) Tùy chọn này xác định khoảng thời gian chờ theo đó tập hợp sẽ được đóng với "điều kiện đóng" trước khi bộ bấm giờ đóng tập hợp. Phạm vi từ **0** đến **100** ms. Mặc định là **3**.

Min. Size of Packet in Aggregation (Kích cỡ Tối thiểu của Gói tin trong Tập hợp) Tùy chọn này xác định kích cỡ tối thiểu của các gói tin được tích lũy trong tập hợp (the byte). Phạm vi từ **0** đến **1500**. Mặc định là **10**.

ADDBA Timeout (Thời gian chờ ADDBA) Tùy chọn này xác định khoảng thời gian sau đó cài đặt ADDBA sẽ chấm dứt, nếu không có trao đổi khung trong khoảng thời gian này theo thỏa thuận Xác nhận Khối (ACK). Phạm vi từ **0** đến **65535** ms. Giá trị mặc định là **0**, đây là giá trị tắt tính năng thời gian chờ .

Aggregation Window Size (Kích cỡ Cửa sổ Tập hợp) Tùy chọn này xác định số gói tin tối đa được truyền mà không cần nhận ACK. Phạm vi từ **0** đến **64**. Mặc định là **64**.

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Voice (Thoại)

Use Aggregation (Sử dụng Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có thiết lập một phiên Thêm Xác nhận theo Khối (ADDBA). Mặc định là **Yes** (Có). Chọn **No** (Không) để tắt tùy chọn này.

Accept Aggregation (Chấp nhận Tập hợp) Tùy chọn này xác định liệu lớp Kiểm soát Truy cập Phương tiện (MAC) có chấp nhận yêu cầu ADDBA. Mặc định là **Yes** (Có). Chọn **No** (Không) để tắt tùy chọn này.

Max. Number of Packets in Aggregation (Số Gói tin Tối đa trong Tập hợp) Tùy chọn này xác định số gói tin tối đa (khung phụ) trong tập hợp. Phạm vi từ **0** đến **2**. Mặc định là **2**.

Max. Aggregation Size (Kích cỡ Tối đa của Tập hợp) Tùy chọn này xác định kích cỡ tối đa của tập hợp (the byte). Phạm vi từ **0** đến **16000**. Mặc định là **10000**.

Timeout Internal (Thời gia chờ Nội bộ) Tùy chọn này xác định khoảng thời gian chờ theo đó tập hợp sẽ được đóng với "điều kiện đóng" trước khi bộ bấm giờ đóng tập hợp. Phạm vi từ **0** đến **100** ms. Mặc định là **10**.

Min. Size of Packet in Aggregation (Kích cỡ Tối thiểu của Gói tin trong Tập hợp) Tùy chọn này xác định kích cỡ tối thiểu của các gói tin được tích lũy trong tập hợp (the byte). Phạm vi từ **0** đến **1500**. Mặc định là **10**.

ADDBA Timeout (Thời gian chờ ADDBA) Tùy chọn này xác định khoảng thời gian sau đó cài đặt ADDBA sẽ chấm dứt, nếu không có trao đổi khung trong khoảng thời gian này theo thỏa thuận Xác nhận Khối (ACK). Phạm vi từ **0** đến **65535** ms. Giá trị mặc định là **0**, đây là giá trị tắt tính năng thời gian chờ .

Aggregation Window Size (Kích cỡ Cửa sổ Tập hợp) Tùy chọn này xác định số gói tin tối đa được truyền mà không cần nhận ACK. Phạm vi từ **0** đến **64**. Mặc định là **64**.

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Wireless (Không dây) > Advanced Wireless Settings (Cài đặt Không dây Nâng cao)

Cấu hình các chức năng không dây nâng cao của cầu nối. Các cài đặt này chỉ nên để một quản trị viên có chuyên môn điều chỉnh vì cài đặt không chính xác có thể làm giảm hiệu suất không dây.



LƯU Ý
Cài đặt trên màn hình *Advanced Wireless Settings* (Cài đặt Không dây Nâng cao) được thiết kế chỉ dành cho người dùng nâng cao.

Advanced Wireless (Không dây Nâng cao)

Use LDPC (Sử dụng LDPC) Low-Density Parity-Check Code (LDPC) (Mã Kiểm tra Chẵn Lẻ Mật độ Thấp) bật hoặc tắt việc sửa lỗi để giảm khả năng mất dữ liệu trong các kênh truyền bị nhiễu. Thuật toán Thích ứng Tốc độ tự động tắt mã hóa LDPC khi làm việc ở các tốc độ PHY cao (cao hơn162). Để sử dụng chương trình sửa lỗi nâng cao LDCP, hãy giữ nguyên giá trị mặc định, **Yes** (Có). Nếu không chọn **No** (Không).

ERP Protection Type (Loại Bảo vệ ERP) Tùy chọn này cấu hình bảo vệ các gói tin OFDM bất kể sự xuất hiện các trạm phát sóng 802.11b trong mạng không dây. Bằng cách gửi các gói tin CTS2Seft hoặc RTS/CTS trong tốc độ 802.11b, cầu nối thông báo cho mạng không dây rằng các gói tin OFDM đang được truyền đi và bảo vệ các gói tin này trong mạng không dây. Các gói tin tin CTS2Self hoặc RTS/CTS tạo phí tổn điều khiển và điều này có thể dẫn đến thông lượng thấp hơn.

Tùy chọn RTS/CTS cung cấp mức phủ sóng tốt hơn nhưng thông lượng lại thấp hơn so với CTS2Self, vì tùy chọn RTS/CTS có bao gồm xác nhận từ thiết bị nhận. Để sử dụng tùy chọn RTS/CTS, giữ nguyên giá trị mặc định, **RTS/CTS**. Tùy chọn None (Không có gì) có thể dẫn tới xung đột giữa các gói tin OFDM và CCK. Để sử dụng tùy chọn None, hãy chọn **None** (Không có gì). Để sử dụng tùy chọn CTS2Self, chọn **CTS2Self**.

11n Protection Type (Loại Bảo vệ 11n) Tùy chọn này cấu hình bảo vệ từ các thiết bị Thông lượng không Cao (HT) có trong mạng không dây. Khi bộ định tuyến không dây (hoặc điểm truy cập) phát hiện thấy có sự kết hợp của thiết bị kế thừa không có thông lượng cao, bộ định tuyến sẽ báo hiệu tất cả các thiết bị HT sử dụng cơ chế RTS/CTS hoặc CTS2Self trước mỗi lần truyền dữ liệu. Tính năng này cũng hỗ trợ bảo vệ chuẩn 802.11n, bao gồm MIMO.

Tùy chọn RTS/CTS cung cấp mức phủ sóng tốt hơn nhưng thông lượng lại thấp hơn so với CTS2Self, vì tùy chọn RTS/CTS có bao gồm xác nhận từ thiết bị nhận. Để sử dụng tùy chọn RTS/CTS, giữ nguyên giá trị mặc định, **RTS/CTS**. Tùy chọn None (Không có gì) có thể dẫn tới xung đột giữa các gói tin kế thừa và HT. Để sử dụng tùy chọn None, hãy chọn **None** (Không có gì). Để sử dụng tùy chọn CTS2Self, chọn **CTS2Self**.

Percentage of maximal transmit power (Tỉ lệ phần trăm công suất truyền tối đa) Tùy chọn này cài đặt tỉ lệ phần trăm công suất truyền tối đa liên quan tới các hạn chế miền theo quy định. Ví dụ, nếu các hạn chế miền theo quy định cho phép truyền tối đa 20 dB, thì cài đặt tỉ lệ 50% cho phép công suất truyền tối đa là 10 dB. Chọn tỉ lệ phần trăm bạn muốn sử dụng **12%**, **25%**, **50%**, hoặc **100%**. Mặc định là **100%**.

QoS Classification Type (Loại Phân loại QoS) Tùy chọn này cài 802.1D hoặc 802.1Q ánh xạ từ trường IP DSCP/TOS đến các ưu tiên của WMM (Background (Nền), Best Effects (Hiệu ứng tốt nhất), Video và Voice (Thoại)). Giữ nguyên giá trị mặc định, **802.1D**, hoặc chọn **802.1Q** mà một số dòng IPTV có sử dụng.

Re-establish Ethernet connection when initiating wireless connection (Thiết lập lại kết nối Ethernet khi bắt đầu kết nối không dây) Để kích hoạt việc phát hiện DHCP từ thiết bị nằm đằng sau cầu nối, cầu nối sẽ cài lại liên kết Ethernet giữa cầu nối và thiết bị mỗi khi kết nối không dây được thiết lập. Để tắt thao tác này, chọn **No** (Không). Nếu không, giữ nguyên giá trị mặc định **Yes** (Có).

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Administration (Quản trị) > Management (Quản lý)

Sử dụng màn hình này để quản lý các chức năng cụ thể của cầu nối: truy cập vào tiện ích dựa trên-web, sao lưu tệp cấu hình và khởi động lại thiết bị.



Management (Quản lý)

Bridge Access (Truy cập Cầu nối)

Sử dụng mật khẩu để bảo vệ truy cập vào tiện ích dựa trên trình duyệt.

Bridge Password (Mật khẩu Cầu nối) Nhập Mật khẩu mới cho cầu nối.

Re-enter to confirm (Nhập lại để xác nhận) Nhập lại Mật khẩu để xác nhận.

Idle Timeout (Thời gian chờ Khi không hoạt động) Đăng nhập sẽ hết thời gian chờ sau khoảng thời gian không hoạt động do bạn chỉ định. Phạm vi từ **60** đến **3600** giây. Mặc định là **600**.

Web Access (Truy cập Web)

Access via Wireless (Truy cập qua Không dây) Nếu bạn đang sử dụng cầu nối trong một miền công cộng và bạn trao quyền truy cập không dây cho khách của mình, bạn có thể tắt truy cập không dây tới tiện ích dựa trên trình duyệt của cầu nối. Bạn chỉ có thể truy cập tiện ích dựa trên trình duyệt qua kết nối có dây nếu bạn tắt cài đặt này. Giữ nguyên giá trị mặc định, **Enabled** (Bật), để cho phép truy cập không dây vào tiện ích dựa trên trình duyệt của cầu nối, hoặc chọn **Disabled** (Tắt) để chặn truy cập không dây vào tiện ích.

Backup and Restore (Sao lưu và Khôi phục)

Backup (Sao lưu) Để sao lưu tệp cấu hình của cầu nối, nhấp **Backup Configurations** (Sao lưu Cấu hình). Sau đó làm theo các hướng dẫn trên màn hình.

Restore (Khôi phục) Nhấp **Browse** (Duyệt) và chọn tệp cấu hình. Sau đó nhấp **Restore Configurations** (Khôi phục Cấu hình).

System Reboot (Khởi động lại Hệ thống)

Reboot (Khởi động lại) Để khởi động hoặc bắt đầu hoạt động lại cho cầu nối, nhấp **Start to Reboot** (Bắt đầu Khởi động lại).

Nhấp **Save Settings** (Lưu Cài đặt) để áp dụng thay đổi, hoặc nhấp **Cancel Changes** (Hủy Thay đổi) để hủy thay đổi của bạn.

Administration (Quản trị) > Factory Defaults (Giá trị Mặc định khi Xuất xưởng)

Sử dụng màn hình này để khôi phục cấu hình của cầu nối về cài đặt mặc định khi xuất xưởng.

Factory Defaults (Giá trị Mặc định khi Xuất xưởng)

Restore All Settings (Khôi phục Tất cả Cài đặt) Để cài lại cài đặt của cầu nối về giá trị mặc định khi xuất xưởng, nhấp **Restore All Settings** (Khôi phục Tất cả Cài đặt). Tất cả cài đặt bạn đã lưu sẽ bị mất khi cài đặt mặc định được khôi phục.



Administration (Quản trị) > Upgrade Firmware (Nâng cấp Phần mềm Hệ thống)

Sử dụng màn hình này để nâng cấp phần mềm hệ thống của cầu nối. Không nâng cấp phần mềm hệ thống nếu bạn không gặp phải trục trặc với cầu nối hoặc phần mềm hệ thống mới có tính năng bạn muốn sử dụng.



Trước khi nâng cấp phần mềm hệ thống, hãy tải tệp nâng cấp phần mềm hệ thống của cầu nối từ trang web của Linksys, **www.Linksys.com/support**.

Upgrade Firmware (Nâng cấp Phần mềm Hệ thống)

Please select a file to upgrade the firmware (Vui lòng chọn một tệp để nâng cấp phần mềm hệ thống) Nhấp **Browse** (Duyệt) và chọn tệp nâng cấp phần mềm hệ thống. Sau đó nhấp **Start to Upgrade** (Bắt đầu Nâng cấp) và làm theo các hướng dẫn trên màn hình.

Status (Trạng thái) > Bridge (Cầu nối)

Thông tin trạng thái hiện tại của cầu nối được hiển thị



Bridge Information (Thông tin về Cầu nối)

Firmware Version (Phiên bản Phần mềm Hệ thống) Hiển thị phiên bản phần mềm hệ thống hiện tại của cầu nối

Local Network (Mạng Nội bộ)

Local MAC Address (Địa chỉ MAC Cục bộ) Hiển thị Địa chỉ MAC của cầu nối như được nhìn thấy trên mạng Ethernet cục bộ của bạn.

IP Address (Địa chỉ IP) Hiển thị Địa chỉ IP của cầu nối như được nhìn thấy trên mạng Ethernet cục bộ của bạn.

Subnet Mask (Mặt nạ Mạng phụ) Hiển thị Mặt nạ Mạng phụ được cấu hình cho mạng cục bộ của bạn.

Status (Trạng thái) > Wireless (Không dây)

Hiển thị thông tin về mạng không dây của bạn.



Wireless (Không dây)

Link Status (Trạng thái Liên kết) Hiển thị trạng thái kết nối với mạng không dây của bạn.

MAC Address (Địa chỉ MAC) Hiển thị Địa chỉ MAC của cầu nối như được nhìn thấy trên mạng không dây cục bộ của bạn.

Network Name (SSID) (Tên Mạng) Hiển thị tên mạng không dây hoặc SSID

BSSID Hiển thị địa chỉ MAC không dây của bộ định tuyến không dây (hoặc điểm truy cập) được kết nối.

Radio Band (Băng tần Radio) Hiển thị băng tần radio của mạng không dây của bạn.

Channel Width (Độ rộng Kênh) Hiển thị độ rộng kênh theo MHz mà mạng không dây của bạn sử dụng.

Wide Channel (Kênh Rộng) Tùy vào cài đặt kênh của bộ định tuyến, Kênh Rộng sẽ hiển thị. Nếu bạn đã chọn Wide - 40MHz Channel (Kênh rộng - 40MHz) cho Băng tần Radio của bộ định tuyến hoặc cài đặt Channel Width (Độ rộng Kênh), kênh này sẽ là kênh Wireless-N chính của bạn.

Standard Channel (Kênh Chuẩn) Hiển thị cài đặt Kênh Chuẩn. Nếu bạn đã chọn Wide - 40MHz Channel (Kênh rộng - 40MHz) cho Băng tần Radio của bộ định tuyến hoặc cài đặt Channel Width (Độ rộng Kênh), Kênh chuẩn sẽ là kênh Wireless-N phụ của bạn.

Bit Rate (Tốc độ Bit) Hiển thị tốc độ truyền dữ liệu.

Signal (Tín hiệu) Hiển thị tỉ lệ phần trăm cường độ tín hiệu. 100% là cường độ tín hiệu mạnh nhất có thể có; 0% là cường độ tín hiệu yếu nhất có thể có.

Security (Bảo mật) Hiển thị chế độ bảo mật mạng không dây của bạn.

Khắc phục sự cố

WES610N/WET610N

Máy tính hay thiết bị Ethernet, có dây khác không thể giao tiếp với bộ định tuyến không dây

1. Truy cập tiện ích dựa trên trình duyệt của cầu nối.
2. Trên màn hình *Basic Wireless Settings* (Cài đặt Không dây Cơ bản), hãy đảm bảo rằng Network Name (SSID) (Tên Mạng) phải khớp với tên mạng không dây của bạn.
3. Hãy đảm bảo rằng cài đặt bảo mật (WPA, WPA2, hoặc WEP) phải khớp với cài đặt bảo mật mạng không dây của bạn.

Cần thay đổi địa chỉ IP của cầu nối.

Nếu cấu nối được nối với mạng bằng máy chủ DHCP (thường là bộ định tuyến mạng), cầu nối sẽ nhận địa chỉ IP của mình từ máy chủ DHCP. Nếu không có máy chủ DHCP, cầu nối sẽ sử dụng địa chỉ IP tĩnh, mặc định là **169.254.1.250**.

Nếu bạn muốn cầu nối luôn sử dụng một địa chỉ IP tĩnh, hãy làm theo các hướng dẫn sau:

1. Truy cập tiện ích dựa trên trình duyệt của cầu nối.
2. Nhấp vào tab **Network Setup** (Cài đặt Mạng).
3. Từ menu thả xuống *Network Connection Type* (Loại Kết nối Internet), chọn **Static IP** (IP tĩnh).
4. Điền đầy đủ vào các trường *Static IP Address* (Địa chỉ IP Tĩnh), *Subnet Mask* (Mặt nạ Mạng phụ) và *Default Gateway* (Cổng Mặc định).
5. Nhấp **Save Settings** (Lưu Cài đặt).

Máy tính hỗ trợ cầu nối hay thiết bị có dây, Ethernet khác sẽ không giao tiếp với thiết bị hỗ trợ không dây khác (như máy tính hay máy in)

Kiểm tra các mục sau:

- Đảm bảo rằng thiết bị hỗ trợ không dây đang ở cùng trong một mạng không dây với máy tính hoặc thiết bị Ethernet, có dây khác được kết nối với cầu nối.
- Đảm bảo bạn sử dụng cùng Network Name (SSID) (Tên mạng) cho tất cả các thiết bị trên mạng không dây.
- Đảm bảo rằng tất cả các thiết bị đều ở trong cùng một mạng IP bằng cách sử dụng các địa chỉ IP tương thích.

Tiện ích dựa trên trình duyệt không chấp nhận mật khẩu của bạn.

Kiểm tra các mục sau:

- Mật khẩu có phân biệt kiểu chữ. Đảm bảo rằng bạn dùng đúng kiểu chữ khi nhập mật khẩu.
- Nếu quên mật khẩu, bạn có thể cài lại cầu nối về giá trị mặc định khi xuất xưởng.

 Bấm và giữ nút **Reset** (Cài lại) của cầu nối trong khoảng 5 giây; mật khẩu sẽ được cài lại về giá trị mặc định khi xuất xưởng, **admin**. Tất cả cài đặt khác của cầu nối cũng sẽ được cài lại về giá trị mặc định khi xuất xưởng. (Để truy cập vào tiện ích dựa trên trình duyệt, hãy nhập **admin** vào trường *Password* (Mật khẩu).)

Sau khi thực hiện thay đổi trong tiện ích dựa trên trình duyệt, cài đặt mới chưa hiển thị trên màn hình

Trên trình duyệt web, hãy nhấp **Refresh** (Làm mới). Nếu cài đặt mới vẫn chưa hiển thị, hãy làm theo các hướng dẫn này

1. Rút bộ thích ứng nguồn ra khỏi cầu nối.
2. Đợi 5 giây rồi cắm lại bộ thích ứng nguồn vào cầu nối.
3. Trên trình duyệt web, hãy nhấp **Refresh** (Làm mới).

WEB
Nếu các thắc mắc của bạn không được đề cập ở đây, hãy tham khảo trang web Linksys tại **Linksys.com/support**

Thông số kỹ thuật

WES610N

Kiểu	WES610N
Chuẩn	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Đèn LED	Nguồn, Ethernet, Wi-Fi Protected Setup™, Không dây, hoạt động và liên kết Ethernet cá nhân
Cổng	Ethernet (4), Nguồn
Nút	Reset (Cài lại), Wi-Fi Protected Setup
Loại cáp	CAT5e
Ăng-ten	3 (trong)
Loại giắc cắm ăng-ten	Không áp dụng
Có thể tháo rời (Có/Không)	Không
Điều biến	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Công suất bức xạ đẳng hướng hiệu dụng (EIRP) theo dBm	802.11a: 15 dBm (quy chuẩn) @ 54Mbps 802.11b: 19 dBm (quy chuẩn) @ 11 Mbps 802.11g: 16 dBm (quy chuẩn) @ 54 Mbps 802.11n (2,4 GHz): 18 dBm (quy chuẩn) @ MCS15 802.11n (5 GHz): 16 dBm (quy chuẩn) @ MCS15
Độ nhạy thu	802.11a: -72 dBm (quy chuẩn) @ 54 Mbps 802.11b: -85 dBm (quy chuẩn) @ 11 Mbps 802.11g: -73 dBm (quy chuẩn) @ 54 Mbps 802.11n (20 MHz): -75 dBm (quy chuẩn) @ MCS15 802.11n (40 MHz): -69 dBm (quy chuẩn) @ MCS15
Độ tăng ích của ăng ten theo dBi	1
Bảo mật Không dây	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit mã khoá bảo mật	Mã hoá tối đa 128-bit

Môi trường

Kích thước	6.97” x 5.04” x 2.68” (177 x 128 x 68 mm)
Trọng lượng	0,65 lb (295 g)
Chứng chỉ	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Nguồn	12V, 1A
Nhiệt độ hoạt động	32 đến 104°F (0 đến 40°C)
Nhiệt độ bảo quản	-4 đến 140°F (-20 đến 60°C)
Độ ẩm hoạt động	10 đến 85% Không ngưng tụ
Độ ẩm bảo quản	5 đến 90% Không ngưng tụ

Thông số kỹ thuật có thể thay đổi mà không báo trước.

WET610N

Kiểu	WET610N
Chuẩn	IEEE 802.3u, 802.11g, 802.11b, 802.11a, 802.11n
Đèn LED	Power, Ethernet, Wi-Fi Protected Setup™, Wireless
Cổng	Ethernet, Nguồn
Nút	Reset (Cài lại), Wi-Fi Protected Setup
Loại cáp	CAT5e
Ăng-ten	3 (trong)
Loại giắc cắm ăng-ten	Không áp dụng
Có thể tháo rời (Có/Không)	Không
Điều biến	802.11a: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11b: CCK/QPSK, BPSK 802.11g: OFDM/BPSK, QPSK, 16-QAM, 64-QAM 802.11n: OFDM/BPSK, QPSK, 16-QAM, 64-QAM
Công suất bức xạ đẳng hướng hiệu dụng (EIRP) theo dBm	802.11a: 15 dBm (quy chuẩn) @ 54Mbps 802.11b: 18 dBm (quy chuẩn) @ 11 Mbps 802.11g: 16 dBm (quy chuẩn) @ 54 Mbps 802.11n: 12 dBm (quy chuẩn) @ 130 Mbps (HT20), 270 Mbps (HT40)
Độ nhạy thu	802.11a: -72 dBm (quy chuẩn) @ 54 Mbps 802.11b: -85 dBm (quy chuẩn) @ 11 Mbps 802.11g: -73 dBm (quy chuẩn) @ 54 Mbps 802.11n: -70 dBm (quy chuẩn) @ MCS15/2.4 GHz, -69 dBm (quy chuẩn) @ MCS15/5.0 GHz
Độ tăng ích của ăng ten theo dBi	1
Bảo mật Không dây	WEP, Wi-Fi Protected Access™ (WPA), Wi-Fi Protected Access™ 2 (WPA2)
Bit mã khoá bảo mật	Mã hoá tối đa 128-bit

Môi trường

Kích thước	5.71” x 4.17” x 2.05” (145 x 106 x 52 mm)
Trọng lượng	5,61 oz (159 g)
Chứng chỉ	FCC, UL/cUL, ICES-003, RSS210, CE, Wi-Fi (IEEE 802 11a/b/g/draft n), WPA2™, Wi-Fi Protected Setup, WMM®
Nguồn	12V, 1A
Nhiệt độ hoạt động	32 đến 104°F (0 đến 40°C)
Nhiệt độ bảo quản	-4 đến 140°F (-20 đến 60°C)
Độ ẩm hoạt động	10 đến 85% Không ngưng tụ
Độ ẩm bảo quản	5 đến 90% Không ngưng tụ

Thông số kỹ thuật có thể thay đổi mà không báo trước.

Linksys.com/support

Cisco, logo Cisco và Linksys là nhãn hiệu hoặc nhãn hiệu đã đăng ký của Cisco và/hoặc các công ty liên kết của Cisco tại Hoa Kỳ và các quốc gia khác.
Bạn có thể tìm thấy danh sách các nhãn hiệu của Cisco tại www.cisco.com/go/trademarks. Tất cả các nhãn hiệu khác được đề cập đến trong tài liệu này là tài sản của các chủ sở hữu tương ứng.

© 2011 Cisco và/hoặc các công ty liên kết của Cisco. Bảo lưu mọi quyền.

3425-01249